Guida per gli sviluppatori

AWS Config

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Config: Guida per gli sviluppatori

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Che cos'è AWS Config? ... 1
Considerazioni ... 1
Modi di utilizzo AWS Config ... 1
Amministrazione delle risorse ... 2
Controllo e conformità ... 2
Gestione e risoluzione dei problemi legati alle modifiche della configurazione ... 2
Analisi di sicurezza ... 2
Soluzioni dei partner ... 3
Funzionalità ... 3
Come AWS Config funziona ... 4
Scoperta delle risorse ... 5
Monitoraggio delle risorse ... 5
Consegna degli elementi di configurazione ... 6
Controlla l'accesso a AWS Config ... 10
Concetti ... 10
AWS Config Interfacce ... 11
Gestione delle risorse ... 12
Registratore della configurazione ... 12
Canale di distribuzione ... 6
AWS Config Regole ... 14
Pacchetti di conformità ... 18
Aggregatori ... 18
Supporto nelle regioni ... 19
Restrizioni dei servizi ... 24
AWS Integrazioni di servizi ... 27
AWS Organizations ... 27
AWS Control Tower ... 27
AWS CloudTrail ... 27
AWS Security Hub ... 27
AWS Audit Manager ... 28
AWS Systems Manager ... 28
AWS Firewall Manager ... 28
Host dedicati di Amazon EC2 ... 29
Application Load Balancer ... 29

AWS CodeBuild ... 29
AWS X-Ray ... 30
AWS Service Management Connector ... 30
Amazon API Gateway ... 30
Informazioni supplementari ... 30
AWS Kit di sviluppo software per AWS Config ... 31
Nozioni di base ... 33
Iscrizione a AWS ... 33
Iscriviti a un Account AWS ... 33
Crea un utente con accesso amministrativo ... 34
Modi per iniziare con AWS Config ... 35
Configurazione AWS Config (console) ... 35
Configurazione ... 35
Configurazione con 1 clic ... 36
Configurazione manuale ... 40
Configurazione AWS Config (AWS CLI) ... 47
Configurazione ... 47
Prerequisiti ... 47
A partire AWS Config ... 108
Verifica ... 119
Lavorare con AWS gli SDK ... 121
Registratore della configurazione ... 123
Gestione del registratore della configurazione (Console) ... 123
Gestione del registratore della configurazione (AWS CLI) ... 124
Rilevamento delle deviazioni del registratore di configurazione ... 128
Canale di distribuzione ... 129
Terminologia ... 130
Aggiornamento del Canale di Distribuzione ... 131
Ridenominazione del Canale di Distribuzione ... 135
Componenti di un elemento di configurazione ... 136
Distribuzione di snapshot di configurazione ... 138
Distribuzione di istantanee di configurazione ... 138
Esempio di istantanea di configurazione da AWS Config ... 139
Verifica dello stato della distribuzione ... 144
Visualizzazione di uno snapshot di configurazione nel bucket Amazon S3 ... 145
Esempi di notifiche ... 146

Esempio notifiche di modifica di un elemento della configurazione 147
Esempio di notifica della distribuzione della cronologia della configurazione 162
Esempio di notifica dell'avvio della distribuzione dello snapshot della configurazione 163
Esempio di notifica della distribuzione dello snapshot della configurazione 163
Esempio di notifica della modifica della conformità 164
Esempio di notifica dell'avvio della valutazione delle regole 168
Esempio di notifica della modifica di un elemento della configurazione sovradimensionato .. 169
Esempio di notifica della distribuzione non conclusa correttamente 170
Gestione delle risorse 172
AWS Config Dashboard 172
Conformità e inventario risorse 173
AWS Config Metriche di utilizzo e successo 175
Tipi di risorsa supportati 177
Amazon AppStream 178
Amazon AppFlow 179
..... 179
Amazon API Gateway 179
Amazon Athena 180
Amazon CloudFront 181
Amazon CloudWatch 181
Amazon CodeGuru 182
Amazon Cognito 182
Amazon Connect 183
Amazon Detective 184
Amazon DynamoDB 184
Amazon EC2 184
Amazon ECR 192
Amazon ECS 192
Amazon EFS 193
Amazon EKS 193
Amazon EMR 194
Amazon EventBridge 194
Amazon Forecast 195
Amazon Fraud Detector 196
Amazon GuardDuty 196
Amazon Inspector 197

Amazon IVS 197
Amazon Keyspaces 197
OpenSearch Servizio Amazon 198
Amazon Personalize 198
Amazon Pinpoint 199
Amazon QLDB 200
Amazon Kendra 200
Amazon Kinesis 200
Amazon Lex 201
Amazon Lightsail 202
Amazon Lookout per le metriche 202
Amazon Lookout per Vision 202
Grafana gestito da Amazon 203
Amazon Managed Service per Prometheus 203
Amazon MemoryDB per Redis 203
Amazon MQ 203
MSK Amazon 204
Amazon Redshift 204
Amazon RDS 206
Amazon Route 53 208
Amazon SageMaker 209
Amazon SES 210
Amazon SNS 211
Amazon SQS 211
Amazon S3 211
Amazon WorkSpaces 213
AWS Amplify 213
AWS AppConfig 213
AWS App Runner 214
AWS App Mesh 215
AWS AppSync 215
AWS Audit Manager 216
AWS Auto Scaling 216
AWS Backup 217
AWS Batch 218
Budget AWS 218

AWS Certificate Manager 218
AWS CloudFormation 219
AWS CloudTrail 219
AWS Cloud9 219
AWS Cloud Map 220
AWS CodeArtifact 220
AWS CodeBuild 221
AWS CodeDeploy 221
AWS CodePipeline 222
AWS Config 222
AWS DMS 223
AWS DataSync 224
AWS Device Farm 225
AWS Elastic Beanstalk 226
AWS FIS 227
AWS Global Accelerator 227
AWS Glue 227
AWS Ground Station 228
AWS HealthLake 228
AWS IAM 229
AWS IoT 230
AWS KMS 233
AWS Lambda 234
AWS Mainframe Modernization 234
AWS Network Firewall 234
AWS Network Manager 235
AWS Panorama 236
AWS Private CA 236
AWS Resilience Hub 237
Esploratore di risorse AWS 237
AWS RoboMaker 238
AWS Signer 238
AWS Secrets Manager 238
AWS Service Catalog 239
AWS Shield 239
AWS Step Functions 240

AWS Systems Manager ... 240
AWS Transfer Family ... 241
AWS WAF ... 241
AWS X-Ray ... 243
Sistema di bilanciamento del carico elastico ... 244
MediaConnect ... 245
MediaPackage ... 245
MediaTailor ... 246
Copertura delle risorse in base alla disponibilità nelle regioni ... 246
Nord e Sud America ... 246
Europa ... 317
Asia Pacifico ... 365
Cina ... 413
Africa e Medio Oriente ... 447
GovCloud ... 495
AWS Risorse per la registrazione ... 539
Considerazioni ... 539
Risorse regionali e globali ... 540
Risorse di registrazione (Console) ... 543
Risorse di registrazione (AWS CLI) ... 547
Frequenza registrazione ... 563
Arresto della registrazione ... 564
Risorse non registrate ... 564
AWS Config Regole e tipi di risorse globali ... 565
Registrazione delle risorse di terze parti ... 566
Fase 1: Configurare l'ambiente di sviluppo ... 567
Fase 2: Modellare la risorsa ... 567
Passaggio 3: Generare gli artefatti ... 570
Passaggio 4: Registrare la risorsa ... 570
Passaggio 5: Pubblicare la configurazione della risorsa ... 570
Registra ed elimina uno stato di configurazione per risorse di terze parti utilizzando AWS CLI ... 571
Gestione di uno stato di configurazione per il tipo di risorsa di terze parti utilizzando le API . 574
Configurazioni software di registrazione ... 574
Visualizzazione delle risorse registrate ... 577
Inventario delle risorse ... 577

Informazioni sulla conformità e risultati della valutazione ... 579
Cronologia di configurazione e conformità ... 592
Tagging delle risorse ... 601
Limitazioni relative al tagging ... 601
Gestione dei tag con le operazioni API AWS Config ... 602
AWS Regole di Config ... 603
Considerazioni sui costi ... 604
Supporto nelle regioni ... 605
Componenti di una regola ... 612
Metadati delle regole ... 613
Struttura delle regole ... 615
Modalità di valutazione ... 633
Tipi di trigger ... 634
Modalità di valutazione ... 635
Valutazioni delle regole ... 639
Regole gestite ... 640
Considerazioni sui costi ... 604
Tipi di trigger ... 641
Modalità di valutazione ... 642
Elenco delle regole gestite di ... 643
Elenco di regole gestite in base alla modalità di valutazione ... 943
Elenco di regole gestite in base al tipo di trigger ... 958
Elenco di regole gestite in base alla disponibilità nelle regioni ... 974
Regole collegate al servizio ... 1310
Creazione di regole gestite conAWS CloudFormation modelli ... 1311
Regole personalizzate ... 1313
Regole di policy personalizzate ... 1313
Regole Lambda personalizzate ... 1314
Considerazioni sui costi ... 604
Tipi di trigger ... 1315
Modalità di valutazione ... 1316
Gestione delle risorse eliminate ... 1317
Creazione di regole di policy personalizzate ... 1319
Creazione di regole Lambda personalizzate ... 1322
Aggiunta, aggiornamento ed eliminazione delle regole ... 1356
Utilizzo della console ... 1356

Utilizzo degli SDK AWS ... 1363
Tramite Security Hub ... 1375
Valutazione delle risorse con le regole ... 1375
Eliminazione dei risultati della valutazione ... 1380
Eliminazione dei risultati della valutazione (console) ... 1380
Eliminazione dei risultati della valutazione (CLI) ... 1381
Eliminazione dei risultati della valutazione (API) ... 1381
Gestione delle regole organizzative ... 1381
Considerazioni ... 1381
Implementazione ... 1383
Supporto nelle regioni ... 1383
Correzione ... 1386
Prerequisito ... 1387
Configurazione della correzione manuale (console) ... 1387
Configurazione della correzione automatica (console) ... 1388
Eliminare l'operazione di correzione (console) ... 1390
Gestione della correzione (API) ... 1390
Supporto nelle regioni ... 1391
Risoluzione dei problemi ... 1395
Pacchetti di conformità ... 1398
Prerequisiti ... 1398
Inizia la registrazione AWS Config ... 1399
Prerequisiti per l'utilizzo di un pacchetto di conformità con correzione ... 1399
Prerequisiti per l'utilizzo di un Conformance Pack con una o più regole AWS Config ... 1399
Prerequisiti per i pacchetti di conformità dell'organizzazione ... 1402
Supporto nelle regioni ... 1404
Controlli di processo ... 1410
Modello di pacchetto di conformità di esempio per la creazione di controlli di processo ... 1411
Inclusione dei controlli di processo in un pacchetto di conformità ... 1412
Modifica dello stato di conformità di un controllo di processo ... 1412
Visualizzazione e modifica del controllo di processo (console) ... 1414
Modelli di esempio di pacchetto di conformità ... 1414
AWSPacchetto di conformità Control Tower Detective Guardrails ... 1419
Best practice operative per ABS CCIG 2.0 Material Workloads ... 1419
Best practice operative per ABS CCIG 2.0 Standard Workloads ... 1646
Best practice operative per ACSC Essentials 8 ... 1815

Best practice operative per ACSC ISM 1842
Best practice operative per IA e ML 1979
Best practice operative per Gateway Amazon API 1979
Best practice operative per Amazon CloudWatch 1980
Best practice operative per Amazon DynamoDB 1980
Best practice operative per Amazon S3 1980
Best practice operative per APRA CPG 234 1980
Best practice operative per la gestione degli asset 2213
Best practice operative per AWS Backup 2213
Best practice operative per la gestione delle AWS identità e degli accessi 2213
Best practice operative per AWS Well-Architected Framework Reliability Pillar 2214
Best practice operative per AWS Well-Architected Framework Security Pillar 2280
Best practice operative per BCP e DR 2439
Best practice operative per BNM RMiT 2440
Best practice operative per il Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile 2779
Best practice operative per CIS AWS Foundations Benchmark v1.4 Level 1 4363
Best practice operative per CIS AWS Foundations Benchmark v1.4 Level 2 4407
Best practice operative per CIS Critical Security Controls v8 IG1 4466
Best practice operative per CIS Critical Security Controls v8 IG2 4569
Best practice operative per CIS Critical Security Controls v8 IG3 4747
Best practice operative per CIS Top 20 4943
Best practice operative per CISA Cyber Essentials 5027
Best practice operative per Criminal Justice Information Services (CJIS) 5243
Best practice operative per CMMC – Livello 1 5382
Best practice operative per CMMC – Livello 2 5508
Best practice operative per CMMC – Livello 3 5820
Best practice operative per CMMC – Livello 4 6276
Best practice operative per CMMC – Livello 5 6769
Best practice operative per CMMC – Livello 1 7334
Best practice operative per CMMC – Livello 2 7458
Best practice operative per servizi di calcolo 7880
Best practice operative per la resilienza dei dati 7881
Best practice operative per servizi di database 7881
Best practice operative per data lake e servizi di analisi 7881
Best practice operative per DevOps 7881

Best practice operative per EC2 7882
Best practice operative per la crittografia e la gestione delle chiavi 7882
Best practice operative per la guida alla cibersicurezza dell'ENISA per le PMI 7882
Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello basso 8042
Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello medio 8154
Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello alto 8279
Best practice operative per FDA Titolo 21 CFR Parte 11 8414
Best practice operative per FedRAMP (Low) 8790
Best practice operative per FedRAMP (Moderato) 9067
Best practice operative per FFIEC 9659
Best practice operative per il Cloud Computing Compliance Criteria Catalog (C5) in Germania 9897
Best practice operative per il Gramm Leach Bliley Act (GLBA) 9986
Best practice operative per GxP dell'UE Allegato 11 10043
Best practice operative per la sicurezza HIPAA 10218
Best practice operative per IRS 1075 10746
Best practice operative per K-ISMS 10985
Best practice operative per il bilanciamento del carico 11075
Best practice operative per la registrazione 11076
Best practice operative per i servizi di gestione e governance 11076
Best practice operative per MAS Notice 655 11076
Best practice operative per MAS TRMG 11119
Best practice operative per il monitoraggio 11355
Best practice operative per NBC TRMG 11356
Best practice operative per NERC CIP BCSI 11854
Best practice operative per i principi di sicurezza cloud NCSC 11926
Best practice operative per NCSC Cyber Assessment Framework 12040
Best practice operative per servizi di rete e distribuzione di contenuti 12235
Best practice operative per NIST 800-53 rev 4 12235
Best practice operative per NIST 800-53 rev 5 12573
Best practice operative per NIST 800 171 13387
Best practice operative per NIST 800 172 13743
Best practice operative per NIST 800 181 13822
Best practice operative per NIST 1800 25 14372
Best practice operative per NIST CSF 14545
Best practice operative per NIST Privacy Framework v1.0 14941

Best practice operative per NYDFS 23 15201
Best practice operative per NZISM 15392
Best practice operative per PCI DSS 3.2.1 15478
Best practice operative per risorse accessibili pubblicamente 15916
Best practice operative per RBI Cyber Security Framework per UCB 15917
Best practice operative per RBI MD-ITF 15969
Best practice operative per servizi di sicurezza, identità e conformità 16133
Best practice operative per serverless 16133
Best practice operative per servizi di archiviazione 16133
Best practice operative per SWIFT CSP 16134
Best practice di sicurezza per Amazon Elastic Container Service (Amazon ECS) 16170
Best practice di sicurezza per Amazon Elastic File System (Amazon EFS) 16170
Best practice di sicurezza per Amazon Elastic Kubernetes Service (Amazon EKS) 16171
Best practice di sicurezza per Amazon CloudFront 16171
Best practice di sicurezza per Amazon OpenSearch Service 16171
Best practice di sicurezza per Amazon Redshift 16171
Best practice di sicurezza per Amazon Relational Database Service (Amazon RDS) 16172
Best practice di sicurezza per AWS Auto Scaling 16172
Best practice di sicurezza per AWS CloudTrail 16172
Best practice di sicurezza per AWS CodeBuild 16172
Best practice di sicurezza per Amazon ECR 16173
Best practice di sicurezza per AWS Lambda 16173
Best practice di sicurezza per AWS Network Firewall 16173
Best practice di sicurezza per Amazon SageMaker 16173
Best practice di sicurezza per AWS Secrets Manager 16174
Best practice di sicurezza per AWS WAF 16174
Modelli di esempio con azione di correzione 16174
Pacchetti di conformità personalizzati 16174
Terminologia 16175
Personalizzazione del modello 16175
Implementazione del pacchetto di conformità personalizzato 16180
Pannello di controllo del pacchetto di conformità 16180
Esplorazione della pagina principale dei pacchetti di conformità 16180
Ulteriori informazioni 16181
Visualizzazione della cronologia di conformità 16181
Visualizzazione della timeline di conformità 16182

Query sulla cronologia di conformità ... 16183
Implementazione di un Conformance Pack (console) ... 16185
Implementa un Conformance Pack utilizzando modelli ... 16185
Modificare un pacchetto di conformità ... 16186
Eliminare un pacchetto di conformità ... 16187
Distribuzione di un pacchetto di conformità (AWS CLI) ... 16187
Distribuire un pacchetto di conformità ... 16188
Visualizzare un pacchetto di conformità ... 16189
Visualizzare lo stato del pacchetto di conformità ... 16190
Visualizzare lo stato di conformità del pacchetto di conformità ... 16190
Ottenere i dettagli di conformità per un pacchetto di conformità specifico ... 16191
Eliminare un pacchetto di conformità ... 16192
Gestione dei pacchetti di conformità (API) ... 16192
Gestione dei pacchetti di conformità organizzativi ... 16193
Considerazioni ... 16193
Implementazione ... 16194
Supporto nelle regioni ... 16195
Risoluzione dei problemi ... 16198
Stato di errore per un pacchetto di conformità ... 16198
Regole diverse in un pacchetto di conformità ... 16199
Aggregatori ... 16202
Casi d'uso ... 16202
Terminologia ... 16203
Come aggregare i dati ... 16203
Supporto nelle regioni ... 16204
Risoluzione dei problemi ... 16208
Pannello di controllo dell'aggregatore ... 16210
Utilizzo del pannello di controllo dell'aggregatore ... 16210
Pannello di controllo della conformità ... 16213
Pannello di controllo dell'inventario ... 16216
Impostazione di un aggregatore (Console) ... 16218
Creazione di un aggregatore ... 16218
Modificare un aggregatore ... 16220
Eliminare un aggregatore ... 16221
Impostazione di un aggregatore (AWS CLI) ... 16221
Aggiungi un aggregatore utilizzando account individuali ... 16222

Aggiunta di un aggregatore utilizzando AWS Organizations 16223
Registrazione di un amministratore delegato 16225
Visualizzare un aggregatore 16227
Modificare un aggregatore 16228
Eliminare un aggregatore 16229
Autorizzazione di account degli aggregatori (console) 16230
Considerazioni 16230
Aggiungi autorizzazione per gli account e le regioni degli aggregatori 16231
Autorizza una richiesta in sospeso per l'account di un aggregatore 16231
Eliminazione dell'autorizzazione per l'account di un aggregatore esistente 16232
Autorizzazione di account degli aggregatori (AWS CLI) 16232
Considerazioni 16233
Aggiungi autorizzazione per gli account e le regioni degli aggregatori 16233
Elimina un account di autorizzazione 16234
Query avanzate 16235
Funzionalità 16236
Componenti della query 16236
Riepilogo 16236
Parametri 16237
Esempi 16237
Query di esempio 16237
Esempi di query sulle relazioni 16243
Limitazioni 16245
Supporto nelle regioni 16248
Editor di query (console) 16252
Considerazioni 16252
Usa una query di AWS esempio 16253
Creazione di una query personalizzata 16254
Editor di query (AWS CLI) 16255
Considerazioni 16255
Query sui dati di configurazione delle risorse 16256
Salvataggio di una query 16257
Visualizzazione di tutte le query salvate 16258
Recupero dei dettagli di una query salvata 16259
Eliminazione di una query salvata 16259
Processore di interrogazioni in linguaggio naturale 16259

Considerazioni ... 16260
Esegui query utilizzando il processore di query in linguaggio naturale ... 16253
Istruzioni di esempio ... 16261
Fornire un feedback ... 16265
Supporto nelle regioni ... 16265
Eliminazione dei dati di ... 16266
Impostazione del periodo di conservazione dei dati (console) ... 16268
Sicurezza ... 16270
Protezione dei dati ... 16271
Crittografia dei dati in transito ... 16272
Crittografia dei dati in transito ... 16272
Identity and Access Management ... 16272
Destinatari ... 16273
Autenticazione con identità ... 16273
Gestione dell'accesso con policy ... 16277
Come AWS Config funziona con IAM ... 16280
Esempi di policy basate su identità ... 16287
AWS politiche gestite ... 16305
Autorizzazioni per il ruolo IAM ... 16453
Aggiornamento del ruolo IAM ... 16457
Autorizzazioni per il bucket Amazon S3 ... 16458
Autorizzazioni per la chiave KMS ... 16463
Autorizzazioni per l'argomento Amazon SNS ... 16466
Risoluzione dei problemi ... 16469
Utilizzo di ruoli collegati ai servizi ... 16471
Risposta agli eventi imprevisti ... 16474
Convalida della conformità ... 16474
Resilienza ... 16475
Sicurezza dell'infrastruttura ... 16476
Analisi della configurazione e delle vulnerabilità ... 16476
Prevenzione del confused deputy tra servizi ... 16476
Best practice ... 16477
Registrazione e monitoraggio ... 16478
Registrazione ... 16478
AWS Config Informazioni in CloudTrail ... 16478
Comprensione delle AWS Config voci dei file di registro ... 16479

Esempio di file di log ... 16480
Monitoraggio ... 16488
Uso di Amazon SQS ... 16488
Usare Amazon EventBridge ... 16490
Endpoint Amazon VPC ... 16496
Crea un endpoint VPC per AWS Config ... 16496
Domande frequenti ... 16497
Non riesco a vedere le mie ultime modifiche alla configurazione ... 16497
Posso aspettarmi di vedere subito le mie modifiche alla configurazione? ... 16497
Relazioni indirette in AWS Config ... 16497
Cos'è la relazione tra risorse? ... 16497
Che cos'è una relazione diretta e indiretta rispetto a una risorsa? ... 16498
Quali relazioni indirette supporta AWS Config ? ... 16498
Come vengono creati gli elementi di configurazione come conseguenza delle relazioni dirette e indirette? ... 16500
Quali sono gli elementi di configurazione generati n base alle relazioni indirette? ... 16500
Come posso recuperare i dati di configurazione relativi alle relazioni indirette? ... 16502
Esempi di codice ... 16504
Azioni ... 16504
`DeleteConfigRule` ... 16505
`DescribeComplianceByConfigRule` ... 16507
`DescribeComplianceByResource` ... 16509
`DescribeConfigRuleEvaluationStatus` ... 16511
`DescribeConfigRules` ... 16513
`DescribeConfigurationRecorderStatus` ... 16516
`DescribeConfigurationRecorders` ... 16517
`DescribeDeliveryChannels` ... 16519
`GetComplianceDetailsByConfigRule` ... 16520
`GetComplianceDetailsByResource` ... 16523
`GetComplianceSummaryByConfigRule` ... 16525
`GetComplianceSummaryByResourceType` ... 16526
`PutConfigRule` ... 16529
`PutDeliveryChannel` ... 16532
Cronologia dei documenti ... 16535
Aggiornamenti precedenti ... 16647
... 16718

Che cos'è AWS Config?

AWS Config fornisce una visualizzazione dettagliata della configurazione delle AWS risorse del tuo AWS account. Questo include le relazioni tra le risorse e la maniera in cui sono state configurate in passato, in modo che tu possa vedere come le configurazioni e le relazioni cambiano nel corso del tempo.

Una AWS risorsa è un'entità su cui puoi lavorare AWS, ad esempio un'istanza Amazon Elastic Compute Cloud (EC2), un volume Amazon Elastic Block Store (EBS), un gruppo di sicurezza o un Amazon Virtual Private Cloud (VPC). Per un elenco completo delle AWS risorse supportate da, consulta. AWS ConfigTipi di risorsa supportati

Considerazioni

- Account AWS: È necessario un dispositivo attivo Account AWS. Per ulteriori informazioni, vedi Iscrizione a AWS.
- Bucket Amazon S3: è necessario un bucket S3 per ricevere i dati per gli snapshot di configurazione e la cronologia. Per ulteriori informazioni, consulta Autorizzazioni per il bucket Amazon S3.
- Argomento di Amazon SNS: è necessario un Amazon SNS per ricevere notifiche in caso di modifiche agli snapshot di configurazione e alla cronologia. Per ulteriori informazioni, consulta l'argomento Autorizzazioni per l'argomento Amazon SNS.
- Ruolo IAM: è necessario un ruolo IAM con le autorizzazioni necessarie per accedere. AWS Config Per ulteriori informazioni, consulta Autorizzazioni per il ruolo IAM.
- Tipi di risorse: puoi decidere quali tipi di risorse vuoi AWS Config registrare. Per ulteriori informazioni, consulta AWS Risorse di registrazione.

Modi di utilizzo AWS Config

Quando si eseguono le applicazioni AWS, in genere si utilizzano AWS risorse che devono essere create e gestite collettivamente. Man mano che la domanda per le applicazioni continua a crescere, aumenta anche la necessità di tenere traccia delle AWS risorse a disposizione. AWS Config è progettato per aiutarvi a supervisionare le risorse delle applicazioni nei seguenti scenari:

Amministrazione delle risorse

Per esercitare una migliore governance sulla configurazione delle risorse e per rilevare le configurazioni errate delle risorse, è necessario un visibilità ad alta granularità sulle risorse esistenti e su come queste risorse sono configurate in ogni momento. È possibile utilizzarlo AWS Config per inviare notifiche ogni volta che vengono create, modificate o eliminate risorse senza dover monitorare queste modifiche, analizzando le chiamate effettuate a ciascuna risorsa.

È possibile utilizzare AWS Config le regole per valutare le impostazioni di configurazione delle AWS risorse. Quando AWS Config rileva che una risorsa viola le condizioni di una delle tue regole, AWS Config contrassegna la risorsa come non conforme e invia una notifica. AWS Config valuta continuamente le risorse man mano che vengono create, modificate o eliminate.

Controllo e conformità

Potresti lavorare con dati che richiedono frequenti verifiche per garantire la conformità con le policy interne e le best practice. Per dimostrare la conformità, è necessario accedere alla cronologia della configurazione delle risorse. Queste informazioni sono fornite da AWS Config.

Gestione e risoluzione dei problemi legati alle modifiche della configurazione

Quando si utilizzano più AWS risorse che dipendono l'una dall'altra, una modifica nella configurazione di una risorsa potrebbe avere conseguenze indesiderate sulle risorse correlate. Con AWS Config, puoi visualizzare in che modo la risorsa che intendi modificare è correlata ad altre risorse e valutare l'impatto della modifica.

Puoi inoltre utilizzare la cronologia della configurazione delle risorse fornito da AWS Config per risolvere i problemi e per accedere all'ultima configurazione valida di una risorsa problematica.

Analisi di sicurezza

Per analizzare i potenziali punti deboli della sicurezza, hai bisogno di informazioni storiche dettagliate sulle configurazioni AWS delle risorse, come le autorizzazioni AWS Identity and Access Management (IAM) concesse ai tuoi utenti o le regole del gruppo di sicurezza di Amazon EC2 che controllano l'accesso alle tue risorse.

Puoi utilizzarla AWS Config per visualizzare la policy IAM assegnata a un utente, gruppo o ruolo in qualsiasi momento durante la registrazione. AWS Config Queste informazioni possono aiutare

a stabilire le autorizzazioni concesse a un utente in un determinato momento: ad esempio, puoi visualizzare se il 1° gennaio 2015 l'utente `John Doe` aveva il permesso di modificare le impostazioni di Amazon VPC.

Puoi anche utilizzarla AWS Config per visualizzare la configurazione dei tuoi gruppi di sicurezza EC2, incluse le regole delle porte aperte in un momento specifico. Queste informazioni sono utili per determinare se un gruppo di sicurezza bloccava il traffico TCP in ingresso su una porta specifica.

Soluzioni dei partner

AWS collabora con specialisti di terze parti in materia di registrazione e analisi per fornire soluzioni che utilizzano l' AWS Config output. Per ulteriori informazioni, visita la pagina dei AWS Config dettagli all'indirizzo AWS Config.

Funzionalità

Durante la configurazione AWS Config, puoi completare quanto segue:

Gestione delle risorse

- Specificate i tipi di risorse che desiderate AWS Config registrare.

- Configura un bucket Amazon S3 per ricevere uno snapshot di configurazione su richiesta e la cronologia di configurazione.
- Configura Amazon SNS per inviare notifiche relative al flusso di configurazione.
- Concedi AWS Config le autorizzazioni necessarie per accedere al bucket Amazon S3 e all'argomento Amazon SNS.

  Per ulteriori informazioni, consulta Visualizzazione AWS delle configurazioni e della cronologia delle risorse e Gestione AWS delle configurazioni e della cronologia delle risorse.

Regole e pacchetti di conformità

- Specificate le regole che desiderate utilizzare AWS Config per valutare le informazioni sulla conformità per i tipi di risorse registrati.
- Utilizza pacchetti di conformità o una raccolta di AWS Config regole e azioni correttive che possono essere implementate e monitorate come un'unica entità all'interno del tuo. Account AWS

Per ulteriori informazioni, consulta Evaluating Resources with AWS Config Rules and Conformance Pack.

Aggregatori

- Utilizza un aggregatore per ottenere una vista centralizzata dell'inventario delle risorse e della conformità. Un aggregatore raccoglie i dati di AWS Config configurazione e conformità da più AWS regioni in un Account AWS unico account e regione.

  Per ulteriori informazioni, consulta Aggregazione di dati multi-regione multi-account.

Query avanzate

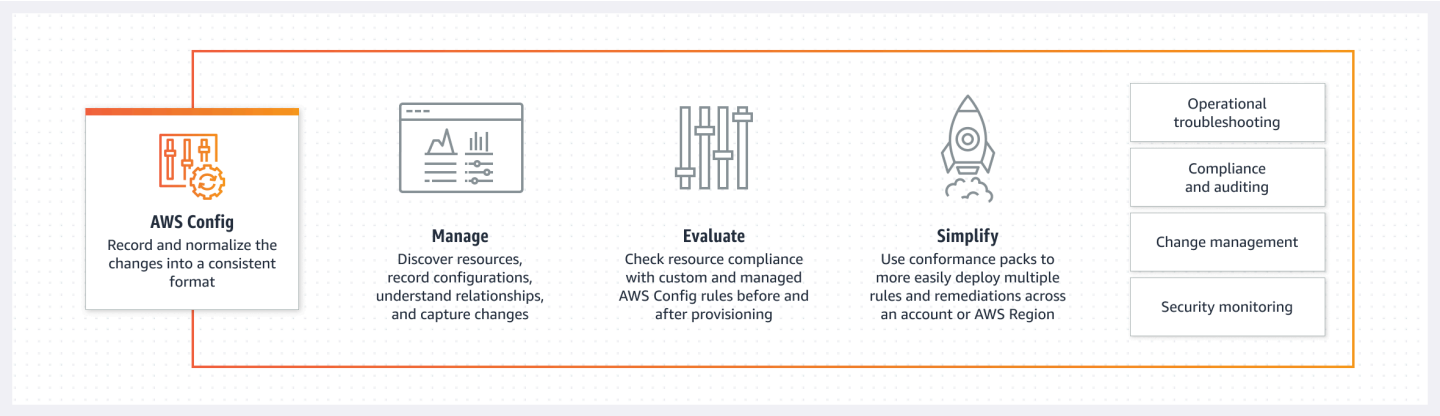
- Usa una delle query di esempio o scrivi la tua query facendo riferimento allo schema di configurazione della risorsa. AWS

  Per ulteriori informazioni, vedere Interrogazione dello stato di configurazione corrente delle AWS risorse.

Come AWS Config funziona

AWS Config fornisce una visualizzazione dettagliata della configurazione delle AWS risorse del tuo AWS account. Questo include le relazioni tra le risorse e la maniera in cui sono state configurate in passato, in modo che tu possa vedere come le configurazioni e le relazioni cambiano nel corso del tempo.

Una AWS risorsa è un'entità su cui puoi lavorare AWS, ad esempio un'istanza Amazon Elastic Compute Cloud (EC2), un volume Amazon Elastic Block Store (EBS), un gruppo di sicurezza o un Amazon Virtual Private Cloud (VPC). Per un elenco completo delle AWS risorse supportate da, consulta. AWS ConfigTipi di risorsa supportati



Scoperta delle risorse

All'attivazione AWS Config, rileva innanzitutto AWS le risorse supportate presenti nel tuo account e genera un elemento di configurazione per ogni risorsa.

AWS Config genera inoltre elementi di configurazione quando la configurazione di una risorsa cambia e conserva i record cronologici degli elementi di configurazione delle risorse dal momento in cui si avvia il registratore di configurazione. Per impostazione predefinita, AWS Config crea elementi di configurazione per ogni risorsa supportata nella regione. Se non desideri AWS Config creare elementi di configurazione per tutte le risorse supportate, puoi specificare i tipi di risorse che desideri vengano monitorati.

Prima di specificare un tipo di risorsa da AWS Config monitorare, controlla la disponibilità della copertura delle risorse per regione per verificare se il tipo di risorsa è supportato nella AWS regione in cui stai effettuando la configurazione AWS Config. Se un tipo di risorsa è supportato da AWS Config almeno una regione, puoi abilitare la registrazione di quel tipo di risorsa in tutte le regioni supportate dalla AWS regione in cui stai AWS Config configurando AWS Config, anche se il tipo di risorsa specificato non è supportato.

Monitoraggio delle risorse

AWS Config tiene traccia di tutte le modifiche alle tue risorse richiamando la chiamata API Descrivi o List per ogni risorsa del tuo account. Il servizio utilizza le stesse chiamate API per acquisire i dettagli della configurazione per tutte le risorse correlate.

Ad esempio, se si rimuove una regola di uscita da un gruppo di sicurezza VPC, viene AWS Config richiamata una chiamata API Descrive sul gruppo di sicurezza. AWS Config quindi richiama una chiamata API Descrivi su tutte le istanze associate al gruppo di sicurezza. Le configurazioni aggiornate del gruppo di sicurezza (la risorsa) e di ciascuna istanza (le risorse correlate) sono

registrate come elementi della configurazione e distribuite in un flusso di configurazione su un bucket Amazon Simple Storage Service (Amazon S3).

AWS Config tiene traccia anche delle modifiche alla configurazione che non sono state avviate dall'API. AWS Config esamina periodicamente le configurazioni delle risorse e genera elementi di configurazione per le configurazioni che sono state modificate.

Se si utilizzano AWS Config regole, valuta AWS Config continuamente le configurazioni AWS delle risorse per verificare le impostazioni desiderate. A seconda della regola, AWS Config valuterà le risorse in risposta alle modifiche di configurazione o periodicamente. Ogni regola è associata a una funzione AWS Lambda , che contiene la logica di valutazione della regola. Quando AWS Config valuta le risorse, richiama la funzione della regola. AWS Lambda La funzione restituisce lo stato di conformità delle risorse valutate. Se una risorsa viola le condizioni di una regola, AWS Config contrassegna la risorsa e la regola come non conformi. Quando lo stato di conformità di una risorsa cambia, AWS Config invia una notifica al tuo argomento Amazon SNS.

Consegna degli elementi di configurazione

AWS Config può fornire gli elementi di configurazione tramite uno dei seguenti canali:

Bucket Amazon S3

AWS Config tiene traccia delle modifiche nella configurazione delle AWS risorse e invia regolarmente dettagli di configurazione aggiornati a un bucket Amazon S3 da te specificato. Per ogni tipo di risorsa AWS Config registrato, invia un file di cronologia della configurazione ogni sei ore. Ogni file cronologia della configurazione contiene i dettagli sulle risorse che sono state modificate in tale periodo di sei ore. Ogni file include risorse di un solo tipo, ad esempio istanze Amazon EC2 o volumi Amazon EBS. Se non viene apportata alcuna modifica alla configurazione, AWS Config non invia un file.

AWS Config invia uno snapshot di configurazione al tuo bucket Amazon S3 quando usi il comando deliver-config-snapshot con la CLI o quando usi AWS l'azione Snapshot con l'API. DeliverConfig AWS Config Uno snapshot di configurazione contiene i dettagli di configurazione per tutte le risorse registrate nel tuo. AWS Config Account AWS Il file della cronologia della configurazione e lo snapshot della configurazione sono in formato JSON.

> **Note**
>
> AWS Config fornisce solo i file di cronologia della configurazione e le istantanee di configurazione al bucket S3 specificato; AWS Config non modifica le politiche del ciclo di

vita per gli oggetti nel bucket S3. Puoi utilizzare policy del ciclo di vita per specificare se desideri eliminare o archiviare gli oggetti in Amazon S3 Glacier. Per ulteriori informazioni, consulta Gestione della configurazione del ciclo di vita nella Guida per l'utente di Amazon Simple Storage Service. Puoi anche consultare il post Archiviazione dei dati Amazon S3 su S3 Glacier sul blog.

Argomento Amazon SNS

Un argomento Amazon Simple Notification Service (Amazon SNS) è un canale di comunicazione che Amazon SNS utilizza per distribuire i messaggi (o le notifiche) verso endpoint di sottoscrizione, ad esempio un indirizzo e-mail o client. Altri tipi di notifiche Amazon SNS includono messaggi di notifica push verso applicazioni su cellulari, notifiche SMS (Short Message Service) verso cellulari e smartphone abilitati e richieste HTTP POST. Per ottenere i risultati migliori, utilizza Amazon SQS come endpoint di notifica per l'argomento SNS ed elabora poi le informazioni contenute nella notifica a livello di programmazione.

AWS Config utilizza l'argomento Amazon SNS che hai specificato per inviarti notifiche. Il tipo di notifica che ricevi è indicato dal valore della chiave `messageType` nel corpo messaggio, come nell'esempio seguente:

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

Le notifiche possono essere uno dei seguenti tipi di messaggi.

Tipo di messaggio	Descrizione
ComplianceChangeNotifica	Il tipo di conformità di una risorsa che AWS Config valuta è cambiato. Il tipo di conformità indica se la risorsa è conforme a una AWS Config regola specifica ed è rappresentato dalla `ComplianceType` chiave del messaggio. Il messaggio include oggetti `newEvaluationResult` e `oldEvaluationResult` per il confronto.
ConfigRulesEvaluationStarted	AWS Config ha iniziato a valutare la regola rispetto alle risorse specificate.

Tipo di messaggio	Descrizione
ConfigurationSnapshotDeliveryStarted	AWS Config ha iniziato a fornire lo snapshot di configurazione al tuo bucket Amazon S3. Il nome del bucket Amazon S3 viene indicato dalla chiave `s3Bucket` nel messaggio.
ConfigurationSnapshotDeliveryCompleted	AWS Config ha inviato con successo lo snapshot di configurazione al tuo bucket Amazon S3.
ConfigurationSnapshotDeliveryFailed	AWS Config non è riuscito a fornire lo snapshot di configurazione al tuo bucket Amazon S3.
ConfigurationHistoryDeliveryCompleted	AWS Config ha inviato con successo la cronologia di configurazione al tuo bucket Amazon S3.
ConfigurationItemChangeNotification	Una risorsa è stata creata, eliminata o modificat a nella configurazione. Questo messaggio include i dettagli dell'elemento di configura zione AWS Config creato per questa modifica e include il tipo di modifica. Queste notifiche vengono distribuiti entro pochi minuti dalla modifica e sono collettivamente note con il nome di flusso di configurazione.

Tipo di messaggio	Descrizione
OversizedConfigurationItemChangeNotification	Questo tipo di messaggio viene recapitato quando la notifica della modifica di un elemento della configurazione supera le dimension i massime consentite da Amazon SNS. Il messaggio include un riepilogo dell'elem ento della configurazione. Ad eccezione dei messaggi SMS, i messaggi Amazon SNS possono contenere fino a 256 KB di dati di testo, tra cui XML, JSON e testo non formattat o. Puoi visualizzare la notifica completa seguendo il percorso del bucket Amazon S3 specificato.
OversizedConfigurationItemChangeDeli veryFailed	AWS Config non è riuscito a inviare la notifica di modifica dell'elemento di configurazione sovradimensionato al tuo bucket Amazon S3.

Per degli esempi di notifiche, consulta Notifiche che AWS Config Invia a un argomento Amazon SNS. Per ulteriori informazioni su Amazon SNS, consultare la Guida per gli sviluppatori di Amazon Simple Notification Service.

> **Note**
>
> Perché non riesco a vedere le mie ultime modifiche alla configurazione?
> AWS Config di solito registra le modifiche alla configurazione delle risorse subito dopo che viene rilevata una modifica o alla frequenza specificata. Tuttavia, questa operazione viene effettuata con il massimo impegno e a volte può richiedere più tempo. Se i problemi persistono dopo qualche tempo, contatta AWS Supporte fornisci i tuoi AWS Config parametri supportati da Amazon. CloudWatch Per informazioni su queste metriche, consulta Metriche di AWS Config utilizzo e successo.

Controlla l'accesso a AWS Config

AWS Identity and Access Management è un servizio Web che consente ai clienti di Amazon Web Services (AWS) di gestire gli utenti e le autorizzazioni degli utenti.

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .
- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Concetti

AWS Config fornisce una visualizzazione dettagliata delle risorse associate all'utente Account AWS, incluso il modo in cui sono configurate, come sono correlate tra loro e come le configurazioni e le loro relazioni sono cambiate nel tempo. Analizziamo più approfonditamente i concetti di AWS Config.

Indice

- AWS Config Interfacce
  - AWS Config Console
  - AWS Config CLI
  - AWS Config API
  - AWS Config SDK
- Gestione delle risorse

- AWS Risorse
- Relazioni tra le risorse
- Registratore della configurazione
- Canale di distribuzione
  - Elementi della configurazione
  - Storico della configurazione
  - Snapshot della configurazione
  - Flusso di configurazione
- AWS Config Regole
  - AWS Config Regole gestite
  - AWS Config Regole personalizzate
  - Tipi di trigger
  - Modalità di valutazione
- Pacchetti di conformità
- Aggregazione di dati multi-regione multi-account
  - Account di origine
  - Regione di origine
  - Aggregatore
  - Account aggregatore
  - Autorizzazione

AWS Config Interfacce

AWS Config Console

È possibile gestire il servizio utilizzando la AWS Config console. Per ulteriori informazioni su AWS Management Console, vedere AWS Management Console.

AWS Config CLI

AWS Command Line Interface È uno strumento unificato con cui puoi interagire AWS Config dalla riga di comando. Per ulteriori informazioni, consulta la Guida per l'utente AWS Command Line Interface. Per un elenco completo dei comandi AWS Config CLI, consulta Comandi disponibili.

AWS Config API

Oltre alla console e alla CLI, puoi anche utilizzare le API AWS Config RESTful per programmare direttamente. AWS Config Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS Config.

AWS Config SDK

In alternativa all'utilizzo dell' AWS Config API, puoi utilizzare uno degli AWS SDK. Ogni SDK include librerie e codice di esempio per piattaforme e linguaggi di programmazione diversi. Gli SDK rappresentano un sistema molto comodo per creare un accesso programmatico a AWS Config. Ad esempio, puoi utilizzare gli SDK per firmare le richieste a livello di crittografia, gestire gli errori e rieseguire automaticamente le richieste. Per ulteriori informazioni, consulta la pagina Strumenti per Amazon Web Services.

Gestione delle risorse

La comprensione dei componenti di base di ti AWS Config aiuterà a tenere traccia dell'inventario e delle modifiche delle risorse e a valutare le configurazioni delle tue AWS risorse.

AWS Risorse

AWS le risorse sono entità che crei e gestisci utilizzando AWS Command Line Interface (CLI), gli AWS SDK o AWS gli strumenti dei partner. AWS Management Console Esempi di AWS risorse includono istanze Amazon EC2, gruppi di sicurezza, Amazon VPC e Amazon Elastic Block Store. AWS Config si riferisce a ciascuna risorsa utilizzando il suo identificatore univoco, come l'ID della risorsa o un Amazon Resource Name (ARN). Per un elenco dei tipi di risorse AWS Config supportati, consulta. Tipi di risorsa supportati

Relazioni tra le risorse

AWS Config rileva AWS le risorse nel tuo account e quindi crea una mappa delle relazioni tra le AWS risorse. Ad esempio, una relazione potrebbe includere un volume `vol-123ab45d` Amazon EBS collegato a un'istanza `i-a1b2c3d4` Amazon EC2 associata al gruppo di sicurezza `sg-ef678hk`.

Per ulteriori informazioni, consulta Tipi di risorsa supportati.

Registratore della configurazione

Il registratore della configurazione memorizza le configurazioni delle risorse supportate nel tuo account come elementi di configurazione. Prima di poter avviare la registrazione, devi creare e

quindi avviare la registrazione della configurazione. Puoi arrestare e riavviare la registrazione della configurazione in qualsiasi momento. Per ulteriori informazioni, consulta Gestione del registratore della configurazione.

Per impostazione predefinita, il registratore di configurazione registra tutte le risorse supportate nella regione in cui AWS Config è in esecuzione. Puoi creare un registratore della configurazione personalizzato che registra solo i tipi di risorse specificati dall'utente. Per ulteriori informazioni, consulta AWS Risorse per la registrazione.

Se utilizzi AWS Management Console o la CLI per attivare il servizio, crea e avvia AWS Config automaticamente un registratore di configurazione per te.

Canale di distribuzione

Poiché registra AWS Config continuamente le modifiche che si verificano alle AWS risorse, invia notifiche e stati di configurazione aggiornati attraverso il canale di distribuzione. È possibile gestire il canale di distribuzione per controllare dove AWS Config inviare gli aggiornamenti di configurazione.

Elementi della configurazione

Un elemento di configurazione rappresenta una point-in-time visualizzazione dei vari attributi di una AWS risorsa supportata presente nel tuo account. I componenti di un elemento di configurazione includono metadati, attributi, relazioni, configurazione corrente ed eventi correlati. AWS Config crea un elemento di configurazione ogni volta che rileva una modifica a un tipo di risorsa che sta registrando. Ad esempio, se AWS Config sta registrando bucket Amazon S3, AWS Config crea un elemento di configurazione ogni volta che un bucket viene creato, aggiornato o eliminato. Puoi anche scegliere di creare un elemento AWS Config di configurazione alla frequenza di registrazione che hai impostato.

Per ulteriori informazioni, consulta Components of a Configuration Item e Scegli quali risorse devono essere registrate | Frequenza di registrazione

Storico della configurazione

Una cronologia della configurazione è una raccolta di elementi della configurazione per una data risorsa durante un qualsiasi periodo di tempo. Una cronologia della configurazione può aiutarti a rispondere a domande relative, ad esempio, a quando la risorsa è stata creata per la prima volta, al modo in cui la risorsa è stata configurata durante l'ultimo mese e alle modifiche della configurazione che sono state apportate ieri alle 9 di mattina. La cronologia delle configurazioni è disponibile in

diversi formati. AWS Config fornisce automaticamente un file di cronologia della configurazione per ogni tipo di risorsa che viene registrato in un bucket Amazon S3 specificato. Puoi selezionare una determinata risorsa nella AWS Config console e passare a tutti gli elementi di configurazione precedenti per quella risorsa utilizzando la sequenza temporale. Inoltre, puoi accedere allo storico degli elementi della configurazione di una risorsa tramite l'API.

Per ulteriori informazioni, vedere Visualizzazione AWS delle configurazioni e della cronologia delle risorse e Gestione AWS delle configurazioni e della cronologia delle risorse.

Snapshot della configurazione

Uno snapshot della configurazione è una raccolta degli elementi della configurazione per tutte le risorse supportate presenti nel tuo account. Questo snapshot della configurazione fornisce un quadro completo delle risorse che vengono registrate e delle loro configurazioni. Lo snapshot della configurazione può essere uno strumento utile per convalidare la configurazione. Ad esempio, puoi esaminare regolarmente lo snapshot della configurazione alla ricerca di risorse che siano state configurate non correttamente o che, potenzialmente, non dovrebbero esistere. Lo snapshot della configurazione è disponibile in più formati. Puoi distribuire lo snapshot della configurazione su un bucket Amazon Simple Storage Service (Amazon S3) di tua scelta. Inoltre, è possibile selezionare un momento nella AWS Config console e navigare nell'istantanea degli elementi di configurazione utilizzando le relazioni tra le risorse.

Flusso di configurazione

Un flusso di configurazione è un elenco aggiornato automaticamente di tutti gli elementi di configurazione per le risorse in fase AWS Config di registrazione. Ogni volta che una risorsa viene creato, modificata o eliminata, AWS Config crea un elemento della configurazione e lo aggiunge al flusso di configurazione. Il flusso di configurazione funziona utilizzando un argomento Amazon Simple Notification Service (Amazon SNS) di tua scelta. Il flusso di configurazione è utile per osservare le modifiche alla configurazione man mano che si verificano in modo da individuare potenziali problemi, generare notifiche se determinate risorse vengono modificate o aggiornare sistemi esterni che devono riflettere la configurazione delle AWS risorse.

AWS Config Regole

Una AWS Config regola rappresenta le impostazioni di configurazione desiderate per AWS risorse specifiche o per un insieme Account AWS. Se una risorsa non supera un controllo delle regole, AWS Config contrassegna la risorsa e la regola come non conformi e ti AWS Config avvisa tramite Amazon SNS. Di seguito sono riportati i possibili risultati di valutazione per una regola: AWS Config

- `COMPLIANT`: la regola supera le condizioni del controllo di conformità.
- `NON_COMPLIANT`: la regola non rispetta le condizioni del controllo di conformità.
- `ERROR`: uno dei parametri richiesti/facoltativi non è valido, non è del tipo corretto o è formattato in modo errato.
- `NOT_APPLICABLE`: utilizzato per filtrare le risorse a cui non può essere applicata la logica della regola. Ad esempio, la regola alb-desync-mode-check verifica solo gli Application Load Balancer e ignora i Network Load Balancer e i Gateway Load Balancer.

Esistono due tipi di regole: regole AWS Config gestite e regole AWS Config personalizzate. Per ulteriori informazioni sulla struttura delle definizioni delle regole e dei metadati delle regole, vedi Componenti di una AWS Config regola.

AWS Config Regole gestite

AWS Config Le regole gestite sono regole predefinite e personalizzabili create da AWS Config. Per un elenco delle regole gestite, vedere Elenco delle regole AWS Config gestite.

AWS Config Regole personalizzate

AWS Config Le regole personalizzate sono regole create da zero. Esistono due modi per creare regole AWS Config personalizzate: con le funzioni Lambda (AWS Lambda Developer Guide) e con Guard (Guard GitHub Repository), un linguaggio. policy-as-code AWS Config le regole personalizzate create con AWS Lambda sono chiamate Regole Lambda AWS Config personalizzate e le regole AWS Config personalizzate create con Guard sono chiamate Regole di policy AWS Config personalizzate.

Per una procedura dettagliata che mostra come creare regole di policy AWS Config personalizzate, vedi Creazione di regole di policy AWS Config personalizzate. Per una procedura dettagliata che mostra come creare regole AWS Config Lambda personalizzate, vedi Creazione di regole Lambda personalizzate AWS Config.

Tipi di trigger

Dopo aver aggiunto una regola al tuo account, AWS Config confronta le tue risorse con le condizioni della regola. Dopo questa valutazione iniziale, AWS Config continua a eseguire le valutazioni ogni volta che ne viene attivata una. I trigger di valutazione sono definiti come parte della regola e possono includere i seguenti tipi.

Tipo di trigger	Descrizione
Modifiche di configurazione	AWS Config esegue le valutazioni della regola quando esiste una risorsa che corrisponde all'ambito della regola e c'è una modifica nella configurazione della risorsa. La valutazione viene eseguita dopo l' AWS Config invio di una notifica di modifica dell'elemento di configura zione. Puoi scegliere le risorse che avviano la valutazione definendo l'ambito della regola. L'ambito può includere quanto segue: • Uno o più tipi di risorse • Una combinazione di un tipo di risorsa e un ID risorsa • Una combinazione di una chiave e un valore di un tag • Quando viene creata, aggiornata o eliminata qualsiasi risorsa registrata AWS Config esegue la valutazione quando rileva una modifica a una risorsa che corrispon de all'ambito della regola. Puoi utilizzare l'ambito per definire le risorse che avviano le valutazioni.
Periodic (Periodico)	AWS Config esegue le valutazioni della regola con una frequenza scelta dall'utente, ad esempio ogni 24 ore.
Ibrido	Alcune regole prevedono sia trigger legati alle modifiche alla configurazione che trigger periodici. Per queste regole, AWS Config valuta le risorse quando rileva una modifica della

Tipo di trigger	Descrizione
	configurazione e anche alla frequenza specifica ta.

Modalità di valutazione

Esistono due modalità di valutazione delle regole. AWS Config

Modalità di valutazione	Descrizione
Proattiva	Utilizza la valutazione proattiva per valutare le risorse prima che vengano implementate. Ciò consente di valutare se un insieme di proprietà della risorsa, se utilizzato per definire una AWS risorsa, sarebbe CONFORME o NON CONFORME, in base all'insieme di regole proattive che hai nel tuo account nella tua regione. Per ulteriori informazioni, consulta Modalità di valutazione. Per un elenco di regole gestite che supportano la valutazione proattiva, vedi Elenco delle regole gestite per modalità di valutazione. AWS Config
Test	Utilizza la valutazione di test per valutare le risorse che sono già state implementate. Ciò consente di valutare le impostazioni di configurazione delle risorse esistenti.

> **Note**
>
> Le regole proattive non correggono le risorse contrassegnate come NON_COMPLIANT e non ne impediscono l'implementazione.

Pacchetti di conformità

Un pacchetto di conformità è una raccolta di AWS Config regole e azioni correttive che possono essere facilmente implementate come singola entità in un account e in una regione o all'interno di un'organizzazione in. AWS Organizations

I pacchetti di conformità vengono creati con un modello YAML contenente l'elenco delle regole AWS Config gestite o personalizzate e le operazioni di correzione. Puoi distribuire il modello utilizzando la console AWS Config o l' AWS CLI.

Per iniziare rapidamente e valutare il tuo AWS ambiente, utilizza uno dei modelli di conformance pack di esempio. Puoi anche creare un file YAML del pacchetto di conformità da zero basandoti su quanto riportato in Pacchetto di conformità personalizzato. Un pacchetto di conformità personalizzato è una raccolta unica di AWS Config regole e azioni correttive che puoi implementare insieme in un account e in una AWS regione o all'interno di un'organizzazione in. AWS Organizations

I controlli di processo sono un tipo di AWS Config regola che consente di tenere traccia delle attività esterne e interne che richiedono la verifica nell'ambito dei pacchetti di conformità. Questi controlli possono essere aggiunti a un pacchetto di conformità esistente o a uno nuovo. È possibile tenere traccia di tutta la conformità, inclusi la AWS Config durata e i controlli manuali, in un'unica posizione.

Aggregazione di dati multi-regione multi-account

L'aggregazione dei dati su più account e più regioni AWS Config consente di aggregare i dati di AWS Config configurazione e conformità di più account e regioni in un unico account. L'aggregazione dei dati su più account e più regioni è utile per gli amministratori IT centrali per monitorare la conformità di più utenti all'interno dell'azienda. Account AWS L'utilizzo degli aggregatori non comporta costi aggiuntivi.

Account di origine

Un account di origine è l'account Account AWS da cui si desidera aggregare i dati di configurazione e conformità AWS Config delle risorse. Un account di origine può essere un account singolo o un'organizzazione in AWS Organizations. Puoi fornire gli account di origine singolarmente o recuperarli tramite. AWS Organizations

Regione di origine

Una regione di origine è la AWS regione da cui si desidera aggregare i dati di AWS Config configurazione e conformità.

Aggregatore

Un aggregatore raccoglie i dati di AWS Config configurazione e conformità da più account e regioni di origine. Crea un aggregatore nella regione in cui desideri visualizzare i dati aggregati di AWS Config configurazione e conformità.

> **Note**
>
> Gli aggregatori forniscono una visualizzazione in sola lettura degli account e delle regioni di origine che l'aggregatore è autorizzato a visualizzare replicando i dati dagli account di origine nell'account di aggregazione. Gli aggregatori non forniscono un accesso mutante a un account o a una regione di origine. Ad esempio, ciò significa che non è possibile distribuire regole tramite un aggregatore o inviare file di istantanee a un account o a una regione di origine tramite un aggregatore.

Account aggregatore

Un account aggregatore è un account all'interno del quale crei un aggregatore.

Autorizzazione

In qualità di proprietario dell'account di origine, l'autorizzazione si riferisce alle autorizzazioni concesse a un account e a una regione di aggregazione per raccogliere i dati di configurazione e conformità. AWS Config L'autorizzazione non è obbligatoria se stai aggregando account di origine che fanno parte di AWS Organizations.

Supporto nelle regioni

> **Note**
>
> Alcune funzionalità di AWS Config sono supportate solo in un sottoinsieme delle AWS regioni in cui AWS Config è supportata.
> Gestione delle risorse
>
> - Per un elenco dei tipi di AWS risorse supportati in quali regioni, vedi Copertura delle risorse per disponibilità regionale.
>
> AWS Config Regole

- Per un elenco delle AWS Config regole supportate in quali regioni, vedi Elenco delle regole AWS Config gestite per disponibilità regionale.
- Per un elenco delle regioni che supportano l'implementazione organizzativa delle AWS Config regole, vedere Organizational Rules | Region Support.
- Per un elenco delle regioni che supportano le azioni di correzione delle AWS Config regole, vedi Remediation Actions | Region Support.

Pacchetti di conformità

- Per un elenco delle regioni che supportano i pacchetti di conformità e la loro implementazione organizzativa, consulta Pacchetti di conformità | Supporto regionale

Aggregatori

- Per un elenco delle regioni che supportano gli aggregatori, consulta Aggregatori | Supporto regionale.

Query avanzate

- Per un elenco delle regioni che supportano le query avanzate, consulta Query avanzate | Supporto regionale.
- Per un elenco di regioni che supportano il processore di query in linguaggio naturale per query avanzate, vedere Elaboratore di query in linguaggio naturale per query avanzate | Region Support.

La tabella seguente elenca le AWS regioni in cui è possibile abilitare. AWS Config

Nome della regione	Regione	Endpoint	Protocollo	
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
		config-fips.us-east-2.amazonaws.com	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Stati Uniti occidentali (California settentrionale)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia Pacifico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pacific (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia Pacifico (Giacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacifico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacifico (Osaka-Locale)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacifico (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacifico (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacifico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Centrale)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Canada occidentale (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Francoforte)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londra)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milano)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Parigi)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spagna)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zurigo)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israele (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Medio Oriente (Bahrein)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (Emirati Arabi Uniti)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Sud America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Restrizioni dei servizi

La tabella seguente descrive le restrizioni all'interno di AWS Config. Salvo diversamente specificato, è possibile richiedere di aumentare le quote. È possibile richiedere un aumento della quota.

Per informazioni sulle altre restrizioni in AWS, consulta Restrizioni dei servizi AWS.

Restrizioni dei servizi AWS Config

Descrizione	Valore restrizione	Può essere aumentata
Numero massimo di regole AWS Config (per regione, per account)	1000	No
Numero massimo di tag per risorsa	50	No

Pacchetti di conformità per account singolo

Descrizione	Valore restrizione	Può essere aumentata
Numero massimo di pacchetti di conformità per account	50	No
Numero massimo di regole AWS Config per pacchetto di conformità	130	No

> **Note**
>
> Le regole AWS Config nei pacchetti di conformità tengono in considerazione il limite del numero massimo di regole AWS Config per regione per account.

Pacchetto di conformità dell'organizzazione

Descrizione	Valore restrizione	Può essere aumentata
Numero massimo di pacchetti di conformità per organizza zione	50	No

Descrizione	Valore restrizione	Può essere aumentata
Numero massimo di regole AWS Config per pacchetto di conformità organizzazione	130	No

> **Note**
>
> L'implementazione a livello di organizzazione tiene in considerazione il limite degli account figlio. Le regole AWS Config nei pacchetti di conformità tengono in considerazione il limite del numero massimo di regole AWS Config per regione per account.

Aggregatori

Descrizione	Valore restrizione	Può essere aumentata
Numero massimo di aggregatori di configurazione	50	Sì
Numero massimo di account in un aggregatore	10000	No
Numero massimo di account aggiunti o cancellati a settimana per tutti gli aggregatori	1000	Sì

Query avanzate

Descrizione	Valore restrizione	Può essere aumentata
Numero massimo di query salvate in un singolo account e in una regione	300	Sì

AWS Integrazioni di servizi con AWS Config

AWS Config supporta integrazioni con diversi altri AWS servizi.

AWS Organizations

È possibile utilizzare AWS Organizations per definire gli account da utilizzare per la funzionalità AWS Config di aggregazione dei dati multi-account e multiregione. AWS Organizations è un servizio di gestione degli account che consente di consolidare più account Account AWS in un'organizzazione da creare e gestire centralmente. Fornendo AWS Organizations i tuoi dati, puoi monitorare lo stato di conformità in tutta l'organizzazione. Per ulteriori informazioni, consulta AWS ConfigAWS Organizations la Guida AWS Organizations per l'utente.

AWS Control Tower

AWS Control Tower AWS Config si attiva su tutti gli account registrati, in modo da poter monitorare la conformità mediante controlli investigativi, registrare le modifiche alle risorse e fornire i registri delle modifiche alle risorse all'account di archiviazione dei registri. Per ulteriori informazioni, consulta Monitorare le modifiche alle risorse AWS Config nella Guida per l'AWS Control Tower utente.

AWS CloudTrail

AWS Config si integra con AWS CloudTrail per correlare le modifiche alla configurazione a particolari eventi del tuo account. Puoi utilizzare CloudTrail i log per ottenere i dettagli dell'evento che ha provocato la modifica, incluso chi ha effettuato la richiesta, a che ora e da quale indirizzo IP. Puoi accedere alla AWS Config timeline dalla CloudTrail console per visualizzare le modifiche alla configurazione relative alle tue AWS attività API.

Per ulteriori informazioni, consulta Logging AWS Config API Calls with AWS CloudTrail nella AWS Config Developer Guide e Creazione di un event data store per gli elementi di AWS Config configurazione con la console nella Guida per l'AWS CloudTrail utente.

AWS Security Hub

AWS Security Hub centralizza i controlli di sicurezza di altri AWS servizi, comprese le regole. AWS Config Security Hub abilita e controlla AWS Config le regole per verificare che le configurazioni delle risorse siano allineate alle best practice. Abilita AWS Config su tutti gli account in tutte le regioni in cui Security Hub deve eseguire controlli di sicurezza sulle risorse del tuo ambiente. Per ulteriori

informazioni, consulta AWS i servizi che inviano i risultati a Security Hub nella Guida per l'AWS Security Hub utente.

AWS Audit Manager

È possibile utilizzare Audit Manager per acquisire le AWS Config valutazioni come prove per gli audit. Quando si crea o si modifica un controllo personalizzato, è possibile specificare una o più AWS Config regole come mappatura della fonte di dati per la raccolta delle prove. AWS Config esegue controlli di conformità in base a queste regole e Audit Manager riporta i risultati come prova del controllo di conformità. Per ulteriori informazioni, consulta la sezione AWS Config Regole supportate da AWS Audit Manager nella Guida AWS Audit Manager per l'utente.

AWS Systems Manager

AWS Config si integra con Systems Manager per registrare le modifiche alla configurazione del software sulle istanze e sui server Amazon EC2 nell'ambiente locale. Con questa integrazione, puoi ottenere visibilità sulle configurazioni del sistema operativo (OS), sugli aggiornamenti a livello di sistema, sulle applicazioni installate, sulla configurazione di rete e altro ancora. AWS Config fornisce inoltre una cronologia delle modifiche alla configurazione a livello di sistema e sistema oltre alle modifiche alla configurazione dell'infrastruttura registrate per le istanze Amazon EC2. Puoi accedere alla AWS Config sequenza temporale dalla console Systems Manager per visualizzare le modifiche alla configurazione delle istanze Amazon EC2 gestite. È possibile utilizzarlo AWS Config per visualizzare la cronologia dell'inventario di Systems Manager e tenere traccia delle modifiche per tutte le istanze gestite.

Per ulteriori informazioni, consulta Integrazione con AWS i servizi | Gestione e governance, registratore di AWS Config configurazione e implementazione del AWS Config Conformance Pack nella Guida per l'utente.AWS Systems Manager

AWS Firewall Manager

Per utilizzare Firewall Manager, è necessario abilitarlo AWS Config per ogni account AWS Organizations membro. Quando vengono create nuove applicazioni, Firewall Manager è il servizio unico per creare regole firewall, creare politiche di sicurezza e applicarle in modo coerente. Per ulteriori informazioni, consulta Enable AWS Config nella AWS WAF AWS Firewall Manager, e AWS Shield Advanced Developer Guide.

> **Note**
>
> Firewall Manager si basa sulla registrazione continua per monitorare le risorse. Se si utilizza Firewall Manager, si consiglia di impostare la frequenza di registrazione su Continuo. Per ulteriori informazioni sulla registrazione continua e sulla registrazione giornaliera, vedere Frequenza di registrazione.

Host dedicati di Amazon EC2

AWS Config si integra con gli host dedicati di Amazon EC2 per valutare la conformità delle licenze. AWS Config registra quando le istanze vengono avviate, interrotte o chiuse su un host dedicato e associa queste informazioni a informazioni a livello di host e istanza relative alle licenze software, come Host ID, ID Amazon Machine Image (AMI), numero di socket e core fisici. Questo ti aiuta a utilizzarli AWS Config come fonte di dati per la reportistica delle licenze. Puoi accedere alla AWS Config timeline dalla console Amazon EC2 Dedicated Hosts per visualizzare le modifiche alla configurazione dei tuoi host dedicati Amazon EC2.

Per ulteriori informazioni, consulta Tieni traccia delle modifiche alla configurazione nella Guida per l'utente di Amazon Elastic Compute Cloud per istanze Linux o Tieni traccia delle modifiche alla configurazione nella Amazon Elastic Compute Cloud User Guide for Windows Instances.

Application Load Balancer

AWS Config si integra con il servizio Elastic Load Balancing (ELB) per registrare le modifiche alla configurazione degli Application Load Balancer. AWS Config include anche le relazioni con i gruppi di sicurezza, i VPC e le sottoreti di Amazon EC2 associati. Puoi utilizzare queste informazioni per l'analisi e la risoluzione dei problemi di sicurezza. Ad esempio, è possibile verificare quali gruppi di sicurezza sono associati all'Application Load Balancer in qualsiasi momento. È possibile accedere alla AWS Config timeline dalla console ELB per visualizzare le modifiche alla configurazione degli Application Load Balancer.

AWS CodeBuild

AWS Config fornisce un inventario delle AWS risorse e una cronologia delle modifiche alla configurazione di tali risorse. AWS Config supporta AWS CodeBuild; come AWS risorsa, il che significa che il servizio può tracciare i tuoi CodeBuild progetti. Per ulteriori informazioni, consulta Use AWS Config with CodeBuild sample nella Guida AWS CodeBuild per l'utente.

AWS X-Ray

AWS X-Ray si integra con AWS Config per registrare le modifiche alla configurazione apportate alle risorse di crittografia X-Ray. È possibile utilizzarlo AWS Config per inventariare le risorse di crittografia a raggi X, controllare la cronologia delle configurazioni a raggi X e inviare notifiche in base alle modifiche delle risorse. Per ulteriori informazioni, consulta Tracciamento delle modifiche alla configurazione della crittografia a raggi X AWS Config nella Guida per gli AWS X-Ray sviluppatori.

AWS Service Management Connector

The AWS Service Management Connector for ServiceNow può sincronizzare AWS Config i dati di più account e regioni utilizzando un aggregatore. Per ulteriori informazioni, consulta Integrazione AWS Config ServiceNow nella Guida per l'AWS Service Management Connector amministratore.

Amazon API Gateway

È possibile utilizzarlo AWS Config per registrare le modifiche alla configurazione apportate alle risorse API API Gateway e inviare notifiche in base alle modifiche delle risorse. Conservare la cronologia delle modifiche eseguite sulla configurazione delle risorse di API Gateway è utile per la risoluzione dei problemi operativi, la revisione e i casi d'uso relativi alla conformità. Per ulteriori informazioni, consulta Monitoring API Gateway API Configuration con AWS Config nella API Gateway Developer Guide.

Informazioni supplementari e risorse correlate

Le seguenti risorse correlate possono rivelarsi utili durante l'utilizzo di questo servizio.

- AWS Config— La pagina web principale per informazioni su AWS Config.
- Prezzi di AWS Config
- Domande frequenti tecniche
- AWS Config Rule Development Kit (RDK): uno strumento open source che consente di configurare AWS Config, creare regole e testarle utilizzando una varietà di tipi di AWS risorse.
- Partner: collegamenti a prodotti dei partner completamente integrati AWS Config per aiutarti a visualizzare, monitorare e gestire i dati dal flusso di configurazione, dalle istantanee di configurazione o dalla cronologia di configurazione.

- Corsi e workshop: collegamenti a corsi specializzati e basati su ruoli, oltre a laboratori di autoapprendimento per aiutarti ad affinare le tue abilità e acquisire esperienza pratica. AWS
- AWS Developer Center: esplora i tutorial, scarica strumenti e scopri gli eventi per sviluppatori. AWS
- AWS Strumenti per sviluppatori: collegamenti a strumenti di sviluppo, SDK, toolkit IDE e strumenti a riga di comando per lo sviluppo e la gestione di applicazioni. AWS
- Centro risorse introduttivo: scopri come configurare Account AWS, entrare a far parte della AWS community e lanciare la tua prima applicazione.
- Tutorial pratici: segui i tutorial per avviare la step-by-step tua prima applicazione su. AWS
- AWS Whitepaper: collegamenti a un elenco completo di AWS white paper tecnici, su argomenti quali architettura, sicurezza ed economia e redatti da Solutions Architects o altri esperti tecnici. AWS
- AWS Support Center: l'hub per la creazione e la gestione dei casi. AWS Support Include anche collegamenti ad altre risorse utili, come forum, domande frequenti tecniche, stato di salute del servizio e AWS Trusted Advisor.
- AWS Support— La pagina web principale per informazioni su AWS Support one-on-one, un canale di supporto a risposta rapida per aiutarti a creare ed eseguire applicazioni nel cloud.
- Contatti - Un punto di contatto centrale per richieste relative a fatturazione, account, eventi, uso illecito e altre questioni relative ad AWS .
- AWS Termini del sito: informazioni dettagliate sul nostro copyright e marchio, sull'account, sulla licenza e sull'accesso al sito e altri argomenti.

AWS Kit di sviluppo software per AWS Config

Un kit di sviluppo AWS software (SDK) semplifica la creazione di applicazioni che accedono a servizi di infrastruttura convenienti, scalabili e affidabili. AWS Con SDK AWS , puoi iniziare in pochi minuti con un pacchetto singolo e scaricabile che include la libreria, esempi di codice e documentazione di riferimento. La tabella seguente elenca gli SDK e le librerie di terze parti disponibili che è possibile utilizzare per accedere a livello di programmazione. AWS Config

Tipo di accesso	Descrizione
AWS SDK	AWS fornisce i seguenti SDK: • AWS Documentazione SDK per C++ • AWS Mobile SDK for iOS Documentazione

Tipo di accesso	Descrizione
	• Documentazione sull'SDK AWS per Go • AWS SDK for Java Documentazione • AWS SDK per la documentazione JavaScript • AWS SDK for .NET Documentazione • AWS SDK for PHP Documentazione • AWS SDK for Python (Boto) Documentazione • AWS SDK for Ruby Documentazione
Librerie di terze parti	Gli sviluppatori della comunità di AWS sviluppatori forniscono anche le proprie librerie, che puoi trovare nei seguenti centri per AWS sviluppatori: • AWS Centro sviluppatori Java • Centro sviluppatori AWS JavaScript • AWS Centro sviluppatori PHP • AWS Python Developer Center • AWS Centro sviluppatori Ruby • AWS Windows e.NET Developer Center

Guida introduttiva con AWS Config

AWS Config fornisce una visualizzazione dettagliata della configurazione delle AWS risorse del tuo Account AWS. Con AWS Config, è possibile esaminare le modifiche nelle configurazioni e nelle relazioni tra le AWS risorse, esplorare la cronologia delle configurazioni delle risorse e utilizzare le regole per determinare la conformità. Per ulteriori informazioni, consulta What Is? AWS Config e come AWS Config funziona.

Iscrizione a AWS

Argomenti

- Iscriviti a un Account AWS
- Crea un utente con accesso amministrativo

Iscriviti a un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center

2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Modi per iniziare con AWS Config

Dopo esserti registrato a Account AWS, puoi iniziare a usare AWS Config la AWS Management Console AWS CLI o gli AWS SDK.

- Configurazione AWS Config con la console
- Configurazione AWS Config con AWS CLI
- Utilizzo AWS Config del servizio con l' AWS SDK

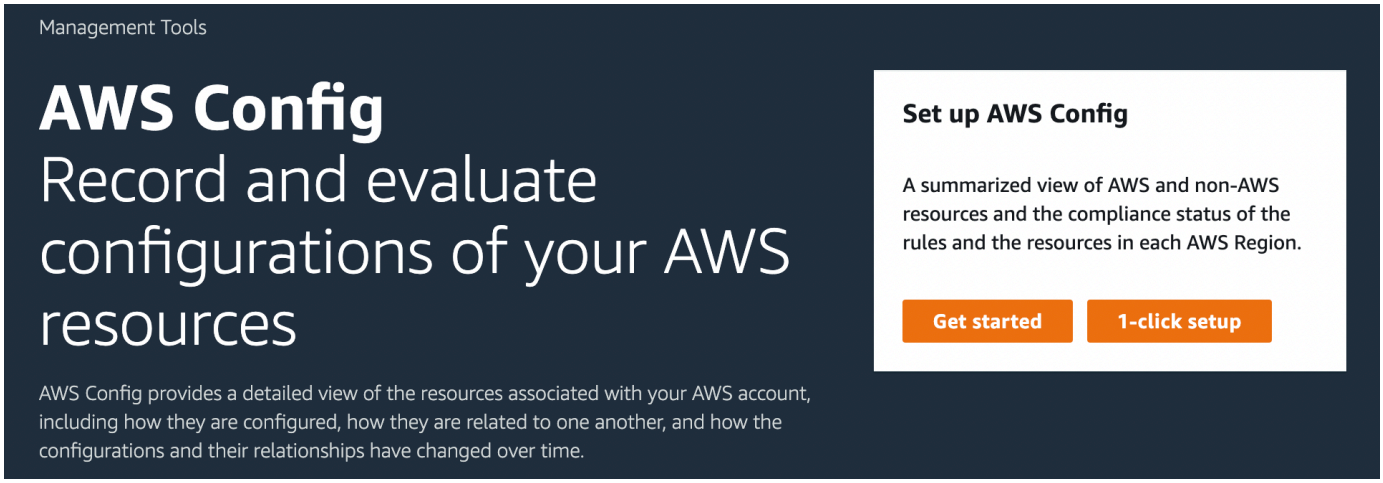
Configurazione AWS Config con la console

AWS Management Console Fornisce un processo di configurazione rapido e semplificato. AWS Config

Configurazione

Per eseguire la configurazione AWS Config con la console

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Se è la prima volta che apri la AWS Config console o la stai configurando AWS Config in una nuova area, la pagina della AWS Config console ha il seguente aspetto:



3. Scegli la configurazione con 1 clic per l'avvio in AWS Config base alle migliori pratiche. AWS Puoi anche scegliere Inizia per eseguire una procedura di configurazione più dettagliata.

Argomenti

- Configurazione con 1 clic
- Configurazione manuale

Configurazione con 1 clic

AWS Config La configurazione in 1 clic aiuta a semplificare la procedura iniziale per i clienti AWS Config della console riducendo il numero di selezioni manuali. Per eseguire tutte le selezioni manuali del processo di configurazione, consulta Configurazione manuale.

Per eseguire la configurazione AWS Config con la console utilizzando la configurazione con 1 clic

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Scegli configurazione con 1 clic.

La pagina di configurazione include tre passaggi, ma tramite il flusso di lavoro di configurazione con 1 clic, verrai indirizzato automaticamente al passaggio 3 (Revisione). Di seguito viene fornita un'analisi dettagliata di tale procedura.

- Impostazioni: per selezionare il modo in cui la AWS Config console registra risorse e ruoli e scegliere dove inviare la cronologia di configurazione e i file degli snapshot di configurazione.

- Regole: per le regioni che supportano le regole, questa sottosezione consente di configurare le regole AWS gestite iniziali che è possibile aggiungere al proprio account.

  Dopo la configurazione, AWS Config valuterà AWS le tue risorse rispetto alle regole che hai scelto. Dopo la configurazione, puoi creare regole aggiuntive e aggiornare quelle esistenti nell'account. Per ulteriori informazioni sulle regole, vedi Gestione delle AWS Config regole.
- Revisione: per verificare i dettagli della configurazione.

Impostazioni

Strategia di registrazione

L'opzione per registrare Tutti i tipi di risorse con sostituzioni personalizzabili è selezionata automaticamente. AWS Config registrerà tutti i tipi di risorse supportate attuali e future in questa regione. Per ulteriori informazioni, consulta Tipi di risorsa supportati.

- Impostazioni predefinite

  La frequenza di registrazione predefinita è impostata su Continuo per te. Ciò significa che AWS Config registra continuamente le modifiche alla configurazione ogni volta che si verifica una modifica.

  AWS Config supporta anche l'opzione di impostare la frequenza di registrazione su Giornaliera. La registrazione giornaliera consente di ricevere un elemento di configurazione (CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza. Per ulteriori informazioni, vedere Frequenza di registrazione.

  > **Note**
  >
  > AWS Firewall Manager dipende dalla registrazione continua per monitorare le risorse. Se si utilizza Firewall Manager, si consiglia di impostare la frequenza di registrazione su Continuo.

- Ignora le impostazioni: opzionale

  Facoltativamente, dopo la configurazione è possibile sovrascrivere la frequenza di registrazione per tipi di risorse specifici o escludere tipi di risorse specifici dalla registrazione. Per ignorare le

impostazioni predefinite, scegli Impostazioni nella barra di navigazione a sinistra della AWS Config console, quindi scegli Modifica.

Considerazioni sulla registrazione delle risorse

Numero elevato di valutazioni AWS Config

Potresti notare una maggiore attività nel tuo account durante la registrazione del mese iniziale con AWS Config rispetto ai mesi successivi. Durante il processo di avvio iniziale, AWS Config esegue valutazioni su tutte le risorse dell'account che hai selezionato per la AWS Config registrazione.

Se esegui carichi di lavoro temporanei, potresti riscontrare un aumento dell'attività di AWS Config dovuto alla registrazione delle modifiche alla configurazione associate alla creazione e all'eliminazione di queste risorse temporanee. Un carico di lavoro temporaneo è un uso temporaneo di risorse di elaborazione che vengono caricate ed eseguite quando necessario. Tra gli esempi vi sono istanze spot di Amazon Elastic Compute Cloud (Amazon EC2), processi Amazon EMR e AWS Auto Scaling. Se desideri evitare l'aumento dell'attività dovuto all'esecuzione di carichi di lavoro temporanei, puoi configurare il registratore di configurazione in modo da escludere questi tipi di risorse dalla registrazione oppure eseguire questi tipi di carichi di lavoro in un account separato con l'opzione AWS Config disattivata per evitare un aumento della registrazione della configurazione e delle valutazioni delle regole.

Tipi di risorse globali | I cluster globali Aurora sono inizialmente inclusi nella registrazione

Il tipo di `AWS::RDS::GlobalCluster` risorsa verrà registrato in tutte le AWS Config regioni supportate in cui è abilitato il registratore di configurazione.

Se non desideri registrare `AWS::RDS::GlobalCluster` in tutte le regioni abilitate, puoi escludere questo tipo di risorsa dalla registrazione dopo la configurazione. Nella barra di navigazione a sinistra, scegli Impostazioni e successivamente Modifica. Da Modifica, vai a Sostituisci impostazioni nella sezione Metodo di registrazione`AWS::RDS::GlobalCluster`, scegli e scegli l'opzione Sostituisci “Escludi dalla registrazione”.

Tipi di risorse globali | I tipi di risorse IAM sono inizialmente esclusi dalla registrazione

“Tutti i tipi di risorse IAM registrati a livello globale” sono inizialmente esclusi dalla registrazione per aiutarti a ridurre i costi. Questo pacchetto include gli utenti IAM, i gruppi, i ruoli e le policy gestite dal cliente. Scegli Rimuovi per rimuovere l'override e includere queste risorse nella registrazione.

L'eccezione a questa nota è per gli Stati Uniti orientali (Virginia settentrionale). I tipi di risorse IAM globali sono inizialmente inclusi nella regione Stati Uniti orientali (Virginia settentrionale) poiché questa regione funge da regione principale per i tipi di risorse IAM globali.

Inoltre, i tipi di risorse IAM globali (`AWS::IAM::UserAWS::IAM::Group`,`AWS::IAM::Role`, e`AWS::IAM::Policy`) non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta Recording AWS Resources | Global Resources.

Governance dei dati

Il periodo di conservazione dei dati predefinito per conservare AWS Config i dati per 7 anni (2557 giorni) è selezionato per te in questa sezione.

L'opzione Usa un ruolo esistente AWS Config collegato al servizio viene selezionata automaticamente e impostata sul ruolo.AWS Config I ruoli collegati al servizio sono predefiniti AWS Config e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi. AWS

Metodo di distribuzione

L'opzione Scegli un bucket dal tuo account è già selezionata in questa sezione. Questa selezione verrà impostata automaticamente sul bucket del tuo account denominato nel formato. `config-bucket-`*`accountid`* Ad esempio, `config-bucket-012345678901`. Se non hai un bucket creato in questo formato, ne verrà creato uno automaticamente. Per creare un bucket, consulta Creazione di un bucket nella Guida per l'utente di Amazon Simple Storage Service.

Per ulteriori informazioni sui bucket S3, consulta Panoramica dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

Regolamento

In questo passaggio, non viene selezionata alcuna regola in Regole gestite di AWS . Ti consigliamo invece di creare e aggiornare le regole dopo aver completato la configurazione dell'account.

Verificare

Controlla i dettagli AWS Config della configurazione. Puoi tornare indietro per regolare le modifiche per ogni sezione. Scegli Conferma per completare la configurazione AWS Config.

Configurazione manuale

Con il flusso di lavoro introduttivo, puoi eseguire tutte le selezioni manuali del processo di configurazione per iniziare a utilizzare la AWS Config console. Per una procedura introduttiva semplificata, consulta Configurazione con 1 clic.

Per eseguire la configurazione AWS Config con la console utilizzando Get started

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Scegli Avvia.

La pagina di configurazione include tre passaggi. Di seguito viene fornita un'analisi dettagliata di tale procedura dopo che hai selezionato Inizia.

- Impostazioni: per selezionare il modo in cui la AWS Config console registra risorse e ruoli e scegliere dove inviare la cronologia di configurazione e i file degli snapshot di configurazione.
- Regole: per le regioni che supportano le regole, questa sottosezione consente di configurare le regole AWS gestite iniziali che è possibile aggiungere al proprio account.

  Dopo la configurazione, AWS Config valuterà AWS le tue risorse rispetto alle regole che hai scelto. Dopo la configurazione, puoi creare regole aggiuntive e aggiornare quelle esistenti nell'account. Per ulteriori informazioni sulle regole, vedi Gestione delle AWS Config regole.
- Revisione: per verificare i dettagli della configurazione.

Impostazioni

Strategia di registrazione

Nella sezione Metodo di registrazione, scegli una strategia di registrazione. È possibile specificare le AWS risorse che si AWS Config desidera registrare.

All resource types with customizable overrides

Imposta AWS Config per registrare le modifiche alla configurazione per tutti i tipi di risorse supportati attuali e futuri in questa regione. È possibile sovrascrivere la frequenza di registrazione per tipi di risorse specifici o escludere tipi di risorse specifici dalla registrazione. Per ulteriori informazioni, consulta Tipi di risorsa supportati.

- Impostazioni predefinite

  Configura la frequenza di registrazione predefinita per tutti i tipi di risorse supportate attuali e future. Per ulteriori informazioni, vedere Frequenza di registrazione.

  - Registrazione continua: AWS Config registrerà le modifiche alla configurazione in modo continuo ogni volta che si verifica una modifica.
  - La registrazione giornaliera consente di ricevere un elemento di configurazione (CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza.

  > **Note**
  >
  > AWS Firewall Manager dipende dalla registrazione continua per monitorare le risorse. Se si utilizza Firewall Manager, si consiglia di impostare la frequenza di registrazione su Continuo.

- Sostituzione delle impostazioni

  Sostituisci la frequenza di registrazione per tipi di risorse specifici o escludi tipi di risorse specifici dalla registrazione. Se cambi la frequenza di registrazione per un tipo di risorsa o interrompi la registrazione per un tipo di risorsa, gli elementi della configurazione già registrati rimarranno invariati.

Specific resource types

Imposta AWS Config per registrare le modifiche alla configurazione solo per i tipi di risorse specificati.

- Tipi di risorsa specifici

  Scegli un tipo di risorsa da registrare e la relativa frequenza. Per ulteriori informazioni, vedere Frequenza di registrazione.

  - Registrazione continua: AWS Config registrerà le modifiche alla configurazione in modo continuo ogni volta che si verifica una modifica.
  - La registrazione giornaliera consente di ricevere un elemento di configurazione (CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza.

> **Note**
>
> AWS Firewall Manager dipende dalla registrazione continua per monitorare le risorse. Se si utilizza Firewall Manager, si consiglia di impostare la frequenza di registrazione su Continuo.

Se cambi la frequenza di registrazione per un tipo di risorsa o interrompi la registrazione per un tipo di risorsa, gli elementi della configurazione già registrati rimarranno invariati.

Considerazioni sulla registrazione delle risorse

Numero elevato di valutazioni AWS Config

Potresti notare una maggiore attività nel tuo account durante la registrazione del mese iniziale con AWS Config rispetto ai mesi successivi. Durante il processo di avvio iniziale, AWS Config esegue valutazioni su tutte le risorse dell'account che hai selezionato per la AWS Config registrazione.

Se esegui carichi di lavoro temporanei, potresti riscontrare un aumento dell'attività di AWS Config dovuto alla registrazione delle modifiche alla configurazione associate alla creazione e all'eliminazione di queste risorse temporanee. Un carico di lavoro temporaneo è un uso temporaneo di risorse di elaborazione che vengono caricate ed eseguite quando necessario. Gli esempi includono istanze Spot Amazon Elastic Compute Cloud (Amazon EC2), lavori Amazon EMR e. AWS Auto Scaling Se vuoi evitare l'aumento dell'attività dovuto all'esecuzione di carichi di lavoro temporanei, puoi configurare il registratore di configurazione per escludere questi tipi di risorse dalla registrazione o eseguire questi tipi di carichi di lavoro in un account separato con AWS Config disattivato per evitare un aumento della registrazione della configurazione e delle valutazioni delle regole.

Considerations: All resource types with customizable overrides

Tipi di risorse globali | I cluster globali Aurora sono inizialmente inclusi nella registrazione

Il tipo di `AWS::RDS::GlobalCluster` risorsa verrà registrato in tutte le AWS Config regioni supportate in cui è abilitato il registratore di configurazione.

Se non desideri registrare `AWS::RDS::GlobalCluster` in tutte le regioni abilitate, scegli "AWS RDS GlobalCluster“ e scegli l'opzione alternativa “Escludi dalla registrazione”.

Tipi di risorse globali | I tipi di risorse IAM sono inizialmente esclusi dalla registrazione

I tipi di risorse IAM globali sono inizialmente esclusi dalla registrazione per aiutarti a ridurre i costi. Questo pacchetto include gli utenti IAM, i gruppi, i ruoli e le policy gestite dal cliente. Scegli Rimuovi per rimuovere l'override e includere queste risorse nella registrazione.

L'eccezione riguarda gli Stati Uniti orientali (Virginia settentrionale). I tipi di risorse IAM globali sono inizialmente inclusi nella regione Stati Uniti orientali (Virginia settentrionale) poiché questa regione funge da regione principale per i tipi di risorse IAM globali.

Inoltre, i tipi di risorse IAM globali (`AWS::IAM::User`AWS::IAM::Group,`AWS::IAM::Role`, e`AWS::IAM::Policy`) non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta Recording AWS Resources | Global Resources.

Limiti

È possibile aggiungere fino a 100 sostituzioni di frequenza e 600 sostituzioni di esclusione.

La registrazione giornaliera non è supportata per i tipi di risorse seguenti:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

Disponibilità nelle regioni

Prima di specificare un tipo di risorsa da AWS Config monitorare, verifica la disponibilità della copertura delle risorse per regione per verificare se il tipo di risorsa è supportato nella AWS regione in cui è stato configurato AWS Config. Se un tipo di risorsa è supportato da AWS Config almeno una regione, puoi abilitare la registrazione di quel tipo di risorsa in tutte le regioni supportate da AWS Config, anche se il tipo di risorsa specificato non è supportato nella AWS regione in cui è stato configurato AWS Config.

Limiti

Nessun limite se tutti i tipi di risorse hanno la stessa frequenza. È possibile aggiungere fino a 100 tipi di risorse con frequenza giornaliera se almeno un tipo di risorsa è impostato su Continuo.

La frequenza giornaliera non è supportata per i tipi di risorse seguenti:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Governance dei dati

- Per Periodo di conservazione dei dati, scegli il periodo di conservazione predefinito per conservare AWS Config i dati per 7 anni (2557) o imposta un periodo di conservazione personalizzato per gli articoli registrati da. AWS Config

  AWS Config ti consente di eliminare i tuoi dati specificando un periodo di conservazione per il tuo. `ConfigurationItems` Quando specifichi un periodo di conservazione, AWS Config conserva il tuo `ConfigurationItems` per quel periodo specificato. Puoi scegliere un periodo compreso tra un minimo di 30 giorni e un massimo di 7 anni (2557 giorni). AWS Config elimina i dati più vecchi del periodo di conservazione specificato.
- Per il ruolo IAM per AWS Config, scegli un ruolo esistente AWS Config collegato al servizio o un ruolo IAM a dal tuo account.
  - I ruoli collegati ai servizi sono predefiniti AWS Config e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi. AWS

    > **Note**
    >
    > Consigliato: utilizza il ruolo collegato al servizio
    > Si consiglia di utilizzare il ruolo collegato al servizio. Un ruolo collegato al servizio aggiunge tutte le autorizzazioni necessarie per AWS Config l'esecuzione prevista.

  - Altrimenti, scegli un ruolo IAM tra uno dei ruoli e delle politiche di autorizzazione preesistenti.

    > **Note**
    >
    > Politiche di autorizzazione per AWS Organizations Can Prevent Acceses
    > Se utilizzi un ruolo IAM preesistente, assicurati che non esista una politica di autorizzazione AWS Organizations che AWS Config impedisca di avere il permesso di registrare le tue risorse. Per ulteriori informazioni sulle politiche di autorizzazione per AWS Organizations, consulta la sezione Gestione delle politiche AWS Organizations nella Guida per l'AWS Organizations utente.
    > Mantieni le autorizzazioni minime quando riutilizzi un ruolo IAM

Se utilizzi un AWS servizio che utilizza AWS Config, come AWS Security Hub o AWS Control Tower, e un ruolo IAM è già stato creato, assicurati che il ruolo IAM che usi durante la configurazione AWS Config mantenga le stesse autorizzazioni minime del ruolo IAM preesistente. È necessario eseguire questa operazione per garantire che l'altro AWS servizio continui a funzionare come previsto.
Ad esempio, se AWS Control Tower dispone di un ruolo IAM che AWS Config consente di leggere oggetti S3, assicurati che vengano concesse le stesse autorizzazioni al ruolo IAM che utilizzi durante la configurazione. AWS Config Altrimenti, potrebbe interferire con il funzionamento AWS Control Tower .

Metodo di distribuzione

- In Metodo di distribuzione, seleziona il bucket S3 a cui AWS Config invia la cronologia della configurazione e i file di snapshot della configurazione:
  - Crea un bucket: digita un nome del bucket S3 nel campo corrispondente.

    Il nome scelto deve essere univoco tra tutti i nomi di bucket esistenti in Amazon S3. Una delle possibilità per garantire l'univocità consiste nell'aggiungere un prefisso, come ad esempio il nome dell'organizzazione. Dopo la creazione, non potrai più modificare il nome del bucket. Per ulteriori informazioni, consulta Restrizioni e limitazioni dei bucket nella Guida per l'utente di Amazon Simple Storage Service.
  - Scegli un bucket dal tuo account: per il campo Nome bucket S3, scegli il bucket preferito.
  - Scegli un bucket da un altro account: digita il nome del bucket S3 nel campo corrispondente.

    > **Note**
    >
    > Autorizzazioni Bucket
    > Se scegli un bucket da un altro account, quel bucket deve avere politiche che concedano le autorizzazioni di accesso a. AWS Config Per ulteriori informazioni, consulta Autorizzazioni per il bucket Amazon S3 per il canale di distribuzione AWS Config.
- Per l'argomento Amazon SNS, scegli Trasmetti modifiche alla configurazione e notifiche su un argomento Amazon SNS per inviare notifiche come la consegna della cronologia di configurazione, la consegna degli snapshot di configurazione e la conformità. AWS Config
- Se hai scelto di trasmettere AWS Config in streaming su un argomento Amazon SNS, scegli l'argomento di destinazione:

- Crea un argomento: in Nome argomento, digita un nome per l'argomento SNS.
- Scegli un argomento dal tuo account: in Nome argomento, seleziona l'argomento preferito.
- Scegli un argomento da un altro account: in ARN argomento, digita il nome della risorsa Amazon (ARN) dell'argomento. Se scegli un argomento da un altro account, l'argomento deve avere politiche che concedano le autorizzazioni di accesso a. AWS Config Per ulteriori informazioni, consulta Autorizzazioni per l'argomento Amazon SNS.

> **Note**
>
> Regione per l'argomento Amazon SNS
> L'argomento Amazon SNS deve esistere nella stessa regione della regione in cui hai effettuato la configurazione. AWS Config

Regolamento

Se stai effettuando la configurazione AWS Config in una regione che supporta le regole, scegli Avanti. Per ulteriori informazioni, consulta Aggiungere, aggiornare ed eliminare regole AWS Config.

Altrimenti, scegli Conferma.

Verificare

Controlla i dettagli della AWS Config configurazione. Puoi tornare indietro per regolare le modifiche per ogni sezione. Scegli Conferma per completare la configurazione AWS Config.

Ulteriori informazioni

Per ulteriori informazioni su come cercare le risorse esistenti nel tuo account e comprendere le configurazioni delle risorse, vedere Visualizzazione delle configurazioni e della cronologia delle risorse di .

Puoi anche utilizzare Amazon Simple Queue Service per monitorare AWS le risorse a livello di codice. Per ulteriori informazioni, consulta Monitoraggio AWS delle modifiche alle risorse con Amazon SQS.

Configurazione con AWS ConfigAWS CLI

AWS CLI È uno strumento unificato per gestire i tuoi servizi. AWS Con un solo strumento da scaricare e configurare, puoi controllare più AWS servizi dalla riga di comando e utilizzare script per automatizzarli. Per ulteriori informazioni sugli strumenti AWS CLI e per istruzioni sull'installazione degli AWS CLI strumenti, vedere quanto segue nella Guida per l'AWS Command Line Interface utente.

- AWS Command Line Interface Guida per l'utente
- Come configurare la AWS Command Line Interface

Se necessario, accedi `aws configure` per AWS CLI configurare l'utilizzo di una AWS regione dove AWS Config disponibile.

Configurazione

Consulta i seguenti argomenti per configurare AWS Config con AWS CLI.

Argomenti

- Prerequisiti
- A partire da AWS ConfigAWS CLI
- Verifica che AWS Config sia stata avviata correttamente con il AWS CLI

Prerequisiti

Prima di eseguire la configurazione AWS con AWS CLI, devi creare un bucket Amazon S3, un argomento Amazon SNS e un ruolo IAM con policy allegate come prerequisiti. Puoi quindi utilizzare il AWS CLI per specificare il bucket, l'argomento e il ruolo per. AWS Config Segui questa procedura per configurare i prerequisiti per AWS Config.

Indice

- Creazione di un bucket Amazon S3
- Creazione di un argomento Amazon SNS
- Creazione di un ruolo IAM

Creazione di un bucket Amazon S3

Se disponi già di un bucket Amazon S3 nell'account e desideri utilizzarlo, puoi ignorare questo passaggio e passare direttamente a Creazione di un argomento Amazon SNS.

Utilizzo della console S3

Per creare un bucket

1. Apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
2. Seleziona Crea bucket.
3. In Bucket name (Nome bucket), immettere un nome conforme a DNS per il bucket.

   Il nome del bucket deve:

   - Essere univoco in tutto Amazon S3.
   - Deve contenere da 3 a 63 caratteri
   - Non contiene caratteri maiuscoli.
   - Iniziare con una lettera minuscola o un numero.

   Una volta creato il bucket, non è possibile modificarne il nome. Assicurati che il nome assegnato al bucket sia univoco tra tutti i nomi di bucket esistenti in Amazon S3. Per ulteriori informazioni sulle regole e le convenzioni di denominazione dei bucket, consulta Restrizioni e limitazioni dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

   > **Important**
   >
   > Evita di includere informazioni sensibili nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.

4. In Regione, scegli la AWS regione in cui desideri che risieda il bucket.

   Scegliere una regione nelle vicinanze per ridurre al minimo la latenza e i costi o rispondere a requisiti normativi. Gli oggetti archiviati in una regione non la lasciano mai a meno che non vengano trasferiti esplicitamente in un'altra regione. Per un elenco delle AWS regioni Amazon S3, consulta gli endpoint AWS di servizio nel. Riferimenti generali di Amazon Web Services

5. In Bucket settings for Block Public Access (Impostazioni bucket per blocco dell'accesso pubblico), scegliere le impostazioni del blocco dell'accesso pubblico che si desidera applicare al bucket.

   Si consiglia di lasciare tutte le impostazioni abilitate, a meno che non si sappia che è necessario disattivarne una o più per il caso d'uso, ad esempio per ospitare un sito Web pubblico. Le impostazioni di blocco dell'accesso pubblico abilitate per il bucket saranno abilitate anche per tutti i punti di accesso creati nel bucket. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta Blocco dell'accesso pubblico di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

6. (Facoltativo) Se si desidera abilitare il Blocco degli oggetti S3:

   a. Scegliere Advanced settings (Impostazioni avanzate) e leggere il messaggio visualizzato.

   > **Important**
   >
   > È possibile abilitare il blocco oggetti S3 per un bucket solo quando lo si crea. Se si abilita il blocco oggetti per il bucket, non è possibile disabilitarlo in un secondo momento. L'abilitazione del blocco oggetti consente anche la funzione Versioni multiple del bucket. Dopo aver abilitato il blocco oggetti per il bucket, è necessario configurare le impostazioni di blocco oggetti prima che tutti gli oggetti nel bucket vengano protetti. Per ulteriori informazioni sulla configurazione della protezione per gli oggetti, consulta Configurazione di Object Lock S3 utilizzando la console Amazon S3.

   b. Se si desidera abilitare il blocco oggetti, immettere abilita nella casella di testo e scegliere Confirm (Conferma).

   Per ulteriori informazioni sulla funzionalità Object Lock S3, consulta Utilizzo di Object Lock S3 nella Guida per l'utente di Amazon Simple Storage Service.

7. Seleziona Crea bucket.

Utilizzo degli SDK AWS

Quando utilizzi gli AWS SDK per creare un bucket, devi creare un client e quindi utilizzare il client per inviare una richiesta di creazione di un bucket. Come best practice, crea il client e il bucket nella

stessa Regione AWS. Se non specifichi una regione quando crei un client o un bucket, Amazon S3 utilizza la regione predefinita Stati Uniti orientali (Virginia settentrionale).

Per creare un client per accedere a un endpoint dual-stack, devi specificare un. Regione AWS Per ulteriori informazioni, consulta Endpoint dual-stack Amazon S3. Per un elenco di quelli disponibili Regioni AWS, consulta Regioni ed endpoint in. Riferimenti generali di AWS

Quando si crea un client, la regione viene mappata all'endpoint specifico della regione. Il client utilizza questo endpoint per comunicare con Amazon S3: `s3.<region>.amazonaws.com`. Se la tua regione è stata lanciata dopo il 20 marzo 2019, il tuo client e il tuo bucket devono trovarsi nella stessa regione. Puoi comunque utilizzare un client nella regione Stati Uniti orientali (Virginia settentrionale) per creare un bucket in qualsiasi regione lanciata prima del 20 marzo 2019. Per ulteriori informazioni, consulta Endpoint legacy.

Questi esempi di codice AWS SDK eseguono le seguenti attività:

- Creazione di un client specificando esplicitamente una Regione AWS - Nell'esempio, il client utilizza l'endpoint `s3.us-west-2.amazonaws.com` per comunicare con Amazon S3. Puoi specificare qualsiasi Regione AWS. Per un elenco di Regioni AWS, consulta Regioni ed endpoint nel Riferimento AWS generale.
- Inviare una richiesta di creazione di bucket specificando solo il nome del bucket - Il client invia ad Amazon S3 la richiesta di creare il bucket nella regione in cui hai creato un client.
- Recupero delle informazioni sulla posizione del bucket - Amazon S3 memorizza le informazioni sulla posizione del bucket nella risorsa secondaria posizione associata al bucket.

I seguenti esempi di codice mostrano come utilizzare`CreateBucket`.

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro da fare GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
        /// <summary>
```

```
        /// Shows how to create a new Amazon S3 bucket.
        /// </summary>
        /// <param name="client">An initialized Amazon S3 client object.</param>
        /// <param name="bucketName">The name of the bucket to create.</param>
        /// <returns>A boolean value representing the success or failure of
        /// the bucket creation process.</returns>
        public static async Task<bool> CreateBucketAsync(IAmazonS3 client, string
bucketName)
        {
            try
            {
                var request = new PutBucketRequest
                {
                    BucketName = bucketName,
                    UseClientRegion = true,
                };

                var response = await client.PutBucketAsync(request);
                return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
            }
            catch (AmazonS3Exception ex)
            {
                Console.WriteLine($"Error creating bucket: '{ex.Message}'");
                return false;
            }
        }
```

Crea un bucket con il blocco degli oggetti abilitato.

```
    /// <summary>
    /// Create a new Amazon S3 bucket with object lock actions.
    /// </summary>
    /// <param name="bucketName">The name of the bucket to create.</param>
    /// <param name="enableObjectLock">True to enable object lock on the
bucket.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateBucketWithObjectLock(string bucketName, bool
enableObjectLock)
    {
        Console.WriteLine($"\tCreating bucket {bucketName} with object lock
{enableObjectLock}.");
```

```
        try
        {
            var request = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true,
                ObjectLockEnabledForBucket = enableObjectLock,
            };

            var response = await _amazonS3.PutBucketAsync(request);

            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine($"Error creating bucket: '{ex.Message}'");
            return false;
        }
    }
```

- Per i dettagli sull'API, consulta la sezione CreateBucket AWS SDK for .NETAPI Reference.

Bash

AWS CLI con lo script Bash

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
```

```
  fi
}

##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

##############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
    echo "  -b bucket_name    The name of the bucket. It must be globally
 unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }
```

```
  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
    usage
    return 1
  fi

  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
  iecho "    Region code:   $region_code"
  iecho ""

  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
```

```
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- Per i dettagli sull'API, consulta CreateBucket AWS CLICommand Reference.

C++

SDK per C++

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
bool AwsDoc::S3::CreateBucket(const Aws::String &bucketName,
                              const Aws::Client::ClientConfiguration
 &clientConfig) {
    Aws::S3::S3Client client(clientConfig);
    Aws::S3::Model::CreateBucketRequest request;
    request.SetBucket(bucketName);

    //TODO(user): Change the bucket location constraint enum to your target
 Region.
    if (clientConfig.region != "us-east-1") {
        Aws::S3::Model::CreateBucketConfiguration createBucketConfig;
        createBucketConfig.SetLocationConstraint(

 Aws::S3::Model::BucketLocationConstraintMapper::GetBucketLocationConstraintForName(
                        clientConfig.region));
        request.SetCreateBucketConfiguration(createBucketConfig);
    }

    Aws::S3::Model::CreateBucketOutcome outcome = client.CreateBucket(request);
    if (!outcome.IsSuccess()) {
```

```
        auto err = outcome.GetError();
        std::cerr << "Error: CreateBucket: " <<
                  err.GetExceptionName() << ": " << err.GetMessage() <<
 std::endl;
    }
    else {
        std::cout << "Created bucket " << bucketName <<
                  " in the specified AWS Region." << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Per i dettagli sull'API, consulta la CreateBucketsezione AWS SDK for C++ API Reference.

CLI

AWS CLI

Esempio 1: creare un bucket

L'`create-bucket`esempio seguente crea un bucket denominato: `my-bucket`

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region us-east-1
```

Output:

```
{
    "Location": "/my-bucket"
}
```

Per ulteriori informazioni, consulta Creare un bucket nella Guida per l'utente di Amazon S3.

Esempio 2: creare un bucket con il proprietario imposto

L'`create-bucket`esempio seguente crea un bucket denominato `my-bucket` che utilizza l'impostazione bucket owner enforced per S3 Object Ownership.

```
aws s3api create-bucket \
```

```
    --bucket my-bucket \
    --region us-east-1 \
    --object-ownership BucketOwnerEnforced
```

Output:

```
{
    "Location": "/my-bucket"
}
```

Per ulteriori informazioni, consulta Controlling ownership of objects and disabling ACLs (Controllo della proprietà degli oggetti e disabilitazione degli ACL) nella Guida per l'utente di Amazon S3.

Esempio 3: creare un bucket al di fuori della regione ``us-east-1``

L'`create-bucket`esempio seguente crea un bucket denominato nella regione. `my-bucket` `eu-west-1` Le aree esterne `LocationConstraint` a `us-east-1` richiedono che venga specificato il valore appropriato per creare il bucket nella regione desiderata.

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region eu-west-1 \
    --create-bucket-configuration LocationConstraint=eu-west-1
```

Output:

```
{
    "Location": "http://my-bucket.s3.amazonaws.com/"
}
```

Per ulteriori informazioni, consulta Creare un bucket nella Guida per l'utente di Amazon S3.

- Per i dettagli sull'API, consulta AWS CLI Command CreateBucketReference.

Go

SDK per Go V2

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3)
 actions
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform
 bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(name string, region string) error {
 _, err := basics.S3Client.CreateBucket(context.TODO(), &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 })
 if err != nil {
  log.Printf("Couldn't create bucket %v in Region %v. Here's why: %v\n",
   name, region, err)
 }
 return err
}
```

- Per i dettagli sull'API, consulta la CreateBucketsezione AWS SDK for Go API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Creare un bucket.

```
import software.amazon.awssdk.core.waiters.WaiterResponse;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.CreateBucketRequest;
import software.amazon.awssdk.services.s3.model.HeadBucketRequest;
import software.amazon.awssdk.services.s3.model.HeadBucketResponse;
import software.amazon.awssdk.services.s3.model.S3Exception;
import software.amazon.awssdk.services.s3.waiters.S3Waiter;
import java.net.URISyntaxException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateBucket {
    public static void main(String[] args) throws URISyntaxException {
        final String usage = """

                Usage:
                    <bucketName>\s

                Where:
                    bucketName - The name of the bucket to create. The bucket
 name must be unique, or an error occurs.
                """;
```

```
        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String bucketName = args[0];
        System.out.format("Creating a bucket named %s\n", bucketName);
        Region region = Region.US_EAST_1;
        S3Client s3 = S3Client.builder()
                .region(region)
                .build();

        createBucket(s3, bucketName);
        s3.close();
    }

    public static void createBucket(S3Client s3Client, String bucketName) {
        try {
            S3Waiter s3Waiter = s3Client.waiter();
            CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
                    .bucket(bucketName)
                    .build();

            s3Client.createBucket(bucketRequest);
            HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
                    .bucket(bucketName)
                    .build();

            // Wait until the bucket is created and print out the response.
            WaiterResponse<HeadBucketResponse> waiterResponse =
 s3Waiter.waitUntilBucketExists(bucketRequestWait);
            waiterResponse.matched().response().ifPresent(System.out::println);
            System.out.println(bucketName + " is ready");

        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

Crea un bucket con il blocco degli oggetti abilitato.

```
    // Create a new Amazon S3 bucket with object lock options.
    public void createBucketWithLockOptions(boolean enableObjectLock, String
 bucketName) {
        S3Waiter s3Waiter = getClient().waiter();
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectLockEnabledForBucket(enableObjectLock)
            .build();

        getClient().createBucket(bucketRequest);
        HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
            .bucket(bucketName)
            .build();

        // Wait until the bucket is created and print out the response.
        s3Waiter.waitUntilBucketExists(bucketRequestWait);
        System.out.println(bucketName + " is ready");
    }
```

- Per i dettagli sull'API, consulta la sezione CreateBucket AWS SDK for Java 2.xAPI Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Crea il bucket.

```
import { CreateBucketCommand, S3Client } from "@aws-sdk/client-s3";

const client = new S3Client({});
```

```
export const main = async () => {
  const command = new CreateBucketCommand({
    // The name of the bucket. Bucket names are unique and have several other
 constraints.
    // See https://docs.aws.amazon.com/AmazonS3/latest/userguide/
bucketnamingrules.html
    Bucket: "bucket-name",
  });

  try {
    const { Location } = await client.send(command);
    console.log(`Bucket created with location ${Location}`);
  } catch (err) {
    console.error(err);
  }
};
```

- Per ulteriori informazioni, consulta la Guida per sviluppatori di AWS SDK for JavaScript.
- Per i dettagli sull'API, consulta la CreateBucketsezione AWS SDK for JavaScript API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun createNewBucket(bucketName: String) {
    val request =
        CreateBucketRequest {
            bucket = bucketName
        }

    S3Client { region = "us-east-1" }.use { s3 ->
        s3.createBucket(request)
        println("$bucketName is ready")
```

```
    }
}
```

- Per i dettagli sull'API, CreateBucketconsulta AWS SDK for Kotlin API reference.

PHP

SDK per PHP

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Creare un bucket.

```
        $s3client = new Aws\S3\S3Client(['region' => 'us-west-2']);

        try {
            $this->s3client->createBucket([
                'Bucket' => $this->bucketName,
                'CreateBucketConfiguration' => ['LocationConstraint' => $region],
            ]);
            echo "Created bucket named: $this->bucketName \n";
        } catch (Exception $exception) {
            echo "Failed to create bucket $this->bucketName with error: " .
 $exception->getMessage();
            exit("Please fix error with bucket creation before continuing.");
        }
```

- Per i dettagli sull'API, consulta la CreateBucketsezione AWS SDK for PHP API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Crea un bucket con le impostazioni di default.

```
class BucketWrapper:
    """Encapsulates S3 bucket actions."""

    def __init__(self, bucket):
        """
        :param bucket: A Boto3 Bucket resource. This is a high-level resource in
 Boto3
                       that wraps bucket actions in a class-like structure.
        """
        self.bucket = bucket
        self.name = bucket.name


    def create(self, region_override=None):
        """
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

        :param region_override: The Region in which to create the bucket. If this
 is
                                not specified, the Region configured in your
 shared
                                credentials is used.
        """
        if region_override is not None:
            region = region_override
        else:
            region = self.bucket.meta.client.meta.region_name
        try:
```

```
            self.bucket.create(CreateBucketConfiguration={"LocationConstraint":
 region})

            self.bucket.wait_until_exists()
            logger.info("Created bucket '%s' in region=%s", self.bucket.name,
 region)
        except ClientError as error:
            logger.exception(
                "Couldn't create bucket named '%s' in region=%s.",
                self.bucket.name,
                region,
            )
            raise error
```

Crea un bucket con versione con una configurazione del ciclo di vita.

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
```

```
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
            }
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )
```

```
    return bucket
```

- Per i dettagli sull'API, consulta CreateBucket AWSSDK for Python (Boto3) API Reference.

Ruby

SDK per Ruby

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
require "aws-sdk-s3"

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                 create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end
```

```
  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      "None. You must create a bucket before you can get its location!"
    else
      @bucket.client.get_bucket_location(bucket:
 @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("doc-example-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

- Per i dettagli sull'API, consulta la CreateBucketsezione AWS SDK for Ruby API Reference.

Rust

SDK per Rust

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
pub async fn create_bucket(
```

```
    client: &Client,
    bucket_name: &str,
    region: &str,
) -> Result<CreateBucketOutput, SdkError<CreateBucketError>> {
    let constraint = BucketLocationConstraint::from(region);
    let cfg = CreateBucketConfiguration::builder()
        .location_constraint(constraint)
        .build();
    client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await
}
```

- Per i dettagli sulle API, consulta la CreateBucketguida di riferimento all'API AWS SDK for Rust.

SAP ABAP

SDK per SAP ABAP

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    TRY.
        lo_s3->createbucket(
            iv_bucket = iv_bucket_name
        ).
        MESSAGE 'S3 bucket created.' TYPE 'I'.
      CATCH /aws1/cx_s3_bucketalrdyexists.
        MESSAGE 'Bucket name already exists.' TYPE 'E'.
      CATCH /aws1/cx_s3_bktalrdyownedbyyou.
        MESSAGE 'Bucket already exists and is owned by you.' TYPE 'E'.
    ENDTRY.
```

- Per i dettagli sulle API, CreateBucketconsulta AWS SDK for SAP ABAP API reference.

Swift

SDK per Swift

> **Note**
>
> Si tratta di una documentazione di pre-rilascio di un SDK nella versione di anteprima. ed è soggetta a modifiche.

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
public func createBucket(name: String) async throws {
    let config = S3ClientTypes.CreateBucketConfiguration(
        locationConstraint: .usEast2
    )
    let input = CreateBucketInput(
        bucket: name,
        createBucketConfiguration: config
    )
    _ = try await client.createBucket(input: input)
}
```

- Per i dettagli sull'API, consulta la CreateBucketguida di riferimento all'API AWS SDK for Swift.

> **Note**
>
> Puoi anche utilizzare un bucket Amazon S3 di un altro account, ma in questo caso potrebbe essere necessario creare una policy che conceda al bucket le autorizzazioni di accesso a AWS Config. Per informazioni sulla concessione di autorizzazioni a un bucket Amazon S3,

consulta Autorizzazioni per il bucket Amazon S3 per il canale di distribuzione AWS Config e vai quindi a Creazione di un argomento Amazon SNS.

Creazione di un argomento Amazon SNS

Se nell'account è già presente un argomento Amazon SNS che desideri utilizzare, puoi ignorare questo passaggio e passare direttamente a Creazione di un ruolo IAM.

Tramite la console SNS

Come creare un argomento Amazon SNS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Esegui una di queste operazioni:
   - Se non è mai stato creato alcun argomento in Account AWS precedenza, leggi la descrizione di Amazon SNS nella home page.
   - Se gli argomenti sono già stati creati sotto il tuo Account AWS nome, nel pannello di navigazione, scegli Argomenti.
3. Nella pagina Topics (Argomenti), seleziona Create new topic (Crea nuovo argomento).
4. Nella pagina Create topic (Crea argomento), nella sezione Details (Dettagli), eseguire queste operazioni:
   a. Per Type (Tipo), scegli un tipo di argomento (standard o FIFO).
   b. Immetti un nome per l'argomento. Per un Argomento FIFO, aggiungere .fifo alla fine del nome.
   c. (Facoltativo) Compilare il Display name (Nome visualizzato) per l'argomento.
   d. (Facoltativo) Per un argomento FIFO, puoi scegliere Deduplicazione dei messaggi basata sul contenuto per abilitare la deduplicazione predefinita dei messaggi. Per ulteriori informazioni, consulta Deduplicazione dei messaggi per argomenti FIFO.
5. (Facoltativo) Espandere la sezione Encryption (Crittografia) e procedere come segue. Per ulteriori informazioni, consultare Crittografia dei dati inattivi.
   a. Scegliere Enable encryption (Abilita crittografia).

b. Specificare la chiave master del cliente (CMK). Per ulteriori informazioni, consulta Termini chiave.

Per ciascun tipo di CMK vengono visualizzati i valori Description (Descrizione), Account e CMK ARN (ARN CMK).

> **Important**
>
> Se non sei il proprietario della CMK, oppure se effettui l'accesso con un account che non dispone delle autorizzazioni `kms:ListAliases` e `kms:DescribeKey`, non puoi visualizzare le informazioni sulla CMK sulla console Amazon SNS.
> Chiedi al proprietario della CMK di riconoscerti queste autorizzazioni. Per esempi e ulteriori informazioni consulta AWS KMS Autorizzazioni API: e Documentazione su operazioni e risorse nella AWS Key Management Service Guida per sviluppatori.

- L'alias/aws/sns della CMK AWS gestita per Amazon SNS (predefinito) è selezionata per impostazione predefinita.

> **Note**
>
> Ricorda quanto segue:
>
> - La prima volta che usi AWS Management Console per specificare la CMK AWS gestita per Amazon SNS per un argomento AWS KMS , crea AWS la CMK gestita per Amazon SNS.
> - In alternativa, la prima volta che utilizzi l'`Publish`azione su un argomento con SSE abilitato, AWS KMS crea la CMK AWS gestita per Amazon SNS.

- Per utilizzare una CMK personalizzata Account AWS, scegli il campo Customer master key (CMK), quindi scegli la CMK personalizzata dall'elenco.

> **Note**
>
> Per istruzioni sulla creazione di CMK personalizzate, consulta Creazione chiavi nella AWS Key Management Service Guida per sviluppatori

- Per utilizzare un ARN CMK personalizzato dal Account AWS tuo o da AWS un altro account, inseriscilo nel campo Customer master key (CMK).

6. (Facoltativo) Per impostazione predefinita, solo il proprietario dell'argomento può pubblicare o sottoscrivere l'argomento. Per configurare autorizzazioni di accesso aggiuntive, espandi la sezione Access policy (Policy di accesso) . Per ulteriori informazioni, consulta Identity and Access Management in Amazon SNS ed Esempi di casi per il controllo degli accessi Amazon SNS.

> **Note**
>
> Quando crei un argomento utilizzando la console, la policy predefinita utilizza la chiave di condizione `aws:SourceOwner`. Questa chiave è analoga a `aws:SourceAccount`.

7. (Facoltativo) Per configurare il modo in cui Amazon SNS riprova a consegnare i messaggi non recapitati, espandere la sezione Delivery retry policy (HTTP/S) (Policy nuovi tentativi di consegna [HTTP/S]). Per ulteriori informazioni, consulta Tentativi di consegna dei messaggi di Amazon SNS.
8. (Facoltativo) Per configurare il modo in cui Amazon SNS registra la consegna dei messaggi CloudWatch, espandi la sezione Registrazione dello stato di consegna. Per ulteriori informazioni, consulta Stato di consegna dei messaggi di Amazon SNS.
9. (facoltativo) Per aggiungere tag di metadati all'argomento, espandere la sezione Tags (Tag), immettere una Key (Chiave) e un Value (Valore) (opzionale) e scegliere Add tag (Aggiungi tag). Per ulteriori informazioni, consulta Assegnazione di tag all'argomento Amazon SNS.
10. Scegli Create topic (Crea argomento).

    L'argomento viene creato e la ***MyTopic***pagina viene visualizzata.

    L'argomento Nome, ARN, (opzionale) Display name (Nome visualizzato), e proprietario dell'argomento's AWS l'ID account viene visualizzato nella sezione Dettagli.
11. Copiare l'ARN dell'argomento negli appunti, ad esempio:

```
arn:aws:sns:us-east-2:123456789012:MyTopic
```

Per sottoscrivere un indirizzo e-mail all'argomento Amazon SNS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.

2. Nel pannello di navigazione sinistro scegli Sottoscrizioni.
3. Nella pagina Sottoscrizioni scegli Crea sottoscrizione.
4. Nella pagina Crea sottoscrizione, nella sezione Dettagli, eseguire queste operazioni:
   a. Per argomento ARN, scegli l'Amazon Resource Name (ARN) di un argomento.
   b. Per Protocollo, scegli un tipo di endpoint. I tipi di endpoint disponibili sono:
      - HTTP/HTTPS
      - Email/Email-JSON
      - Amazon Data Firehose
      - Amazon SQS

        > **Note**
        > Per sottoscrivere ad un argomento SNS FIFO scegli questa opzione.

      - AWS Lambda
      - Endpoint applicazione piattaforma
      - SMS
   c. Per Endpoint, inserisci il valore dell'endpoint, ad esempio un indirizzo e-mail o l'ARN di una coda Amazon SQS.
   d. Solo endpoint Firehose: per il ruolo di sottoscrizione ARN, specifica l'ARN del ruolo IAM che hai creato per la scrittura nei flussi di distribuzione Firehose. Per ulteriori informazioni, consulta gli argomenti Prerequisiti per la sottoscrizione dei flussi di distribuzione di Firehose ad Amazon SNS.
   e. (Facoltativo) Per gli endpoint Firehose, Amazon SQS, HTTP/S, puoi anche abilitare la consegna di messaggi non elaborati. Per ulteriori informazioni, consulta Consegna di messaggi non elaborati Amazon SNS.
   f. (Facoltativo) Per configurare un criterio di filtro, espandere la sezione policy di filtro della sottoscrizione. Per ulteriori informazioni, consulta Policy di filtro degli abbonamenti Amazon SNS.
   g. (Facoltativo) Per configurare una coda DLQ per la sottoscrizione, espandere la sezione Policy di redrive (coda DLQ). Per ulteriori informazioni, consulta Code DLQ (DLQ) Amazon SNS.
   h. Scegli Create Subscription (Crea sottoscrizione).

La console crea la sottoscrizione e apre la pagina dettagli della sottoscrizione.

Utilizzo degli SDK AWS

Per utilizzare un AWS SDK, devi configurarlo con le tue credenziali. Per ulteriori informazioni, consulta File di configurazione e credenziali condivisi nella Guida di riferimento per SDK AWS e strumenti.

I seguenti esempi di codice mostrano come utilizzare. `CreateTopic`

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro da fare GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Crea un argomento con un nome di specifico.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.SimpleNotificationService;
    using Amazon.SimpleNotificationService.Model;

    /// <summary>
    /// This example shows how to use Amazon Simple Notification Service
    /// (Amazon SNS) to add a new Amazon SNS topic.
    /// </summary>
    public class CreateSNSTopic
    {
        public static async Task Main()
        {
            string topicName = "ExampleSNSTopic";

            IAmazonSimpleNotificationService client = new
AmazonSimpleNotificationServiceClient();

            var topicArn = await CreateSNSTopicAsync(client, topicName);
```

```
            Console.WriteLine($"New topic ARN: {topicArn}");
        }

        /// <summary>
        /// Creates a new SNS topic using the supplied topic name.
        /// </summary>
        /// <param name="client">The initialized SNS client object used to
        /// create the new topic.</param>
        /// <param name="topicName">A string representing the topic name.</param>
        /// <returns>The Amazon Resource Name (ARN) of the created topic.</
returns>
        public static async Task<string>
 CreateSNSTopicAsync(IAmazonSimpleNotificationService client, string topicName)
        {
            var request = new CreateTopicRequest
            {
                Name = topicName,
            };

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

Crea un nuovo argomento con un nome e attributi FIFO e di deduplicazione specifici.

```
    /// <summary>
    /// Create a new topic with a name and specific FIFO and de-duplication
 attributes.
    /// </summary>
    /// <param name="topicName">The name for the topic.</param>
    /// <param name="useFifoTopic">True to use a FIFO topic.</param>
    /// <param name="useContentBasedDeduplication">True to use content-based de-
duplication.</param>
    /// <returns>The ARN of the new topic.</returns>
    public async Task<string> CreateTopicWithName(string topicName, bool
 useFifoTopic, bool useContentBasedDeduplication)
    {
        var createTopicRequest = new CreateTopicRequest()
        {
```

```
            Name = topicName,
        };

        if (useFifoTopic)
        {
            // Update the name if it is not correct for a FIFO topic.
            if (!topicName.EndsWith(".fifo"))
            {
                createTopicRequest.Name = topicName + ".fifo";
            }

            // Add the attributes from the method parameters.
            createTopicRequest.Attributes = new Dictionary<string, string>
            {
                { "FifoTopic", "true" }
            };
            if (useContentBasedDeduplication)
            {
                createTopicRequest.Attributes.Add("ContentBasedDeduplication",
"true");
            }
        }

        var createResponse = await
_amazonSNSClient.CreateTopicAsync(createTopicRequest);
        return createResponse.TopicArn;
    }
```

- Per i dettagli sull'API, consulta la CreateTopicsezione AWS SDK for .NET API Reference.

C++

SDK per C++

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
//! Create an Amazon Simple Notification Service (Amazon SNS) topic.
```

```
/*!
  \param topicName: An Amazon SNS topic name.
  \param topicARNResult: String to return the Amazon Resource Name (ARN) for the
 topic.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SNS::createTopic(const Aws::String &topicName,
                              Aws::String &topicARNResult,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SNS::SNSClient snsClient(clientConfiguration);

    Aws::SNS::Model::CreateTopicRequest request;
    request.SetName(topicName);

    const Aws::SNS::Model::CreateTopicOutcome outcome =
 snsClient.CreateTopic(request);

    if (outcome.IsSuccess()) {
        topicARNResult = outcome.GetResult().GetTopicArn();
        std::cout << "Successfully created an Amazon SNS topic " << topicName
                  << " with topic ARN '" << topicARNResult
                  << "'." << std::endl;

    }
    else {
        std::cerr << "Error creating topic " << topicName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
        topicARNResult.clear();
    }

    return outcome.IsSuccess();
}
```

- Per i dettagli sull'API, consulta la CreateTopicsezione AWS SDK for C++ API Reference.

CLI

AWS CLI

Creazione di un argomento SNS

Nell'esempio `create-topic` seguente viene creato un argomento SNS denominato `my-topic`.

```
aws sns create-topic \
    --name my-topic
```

Output:

```
{
    "ResponseMetadata": {
        "RequestId": "1469e8d7-1642-564e-b85d-a19b4b341f83"
    },
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

Per ulteriori informazioni, consulta Using the AWS Command Line Interface with Amazon SQS e Amazon SNS nella Command Line Interface AWS User Guide.

- Per i dettagli sull'API, consulta AWS CLI Command CreateTopicReference.

Go

SDK per Go V2

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
// SnsActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type SnsActions struct {
 SnsClient *sns.Client
}
```

```
// CreateTopic creates an Amazon SNS topic with the specified name. You can
 optionally
// specify that the topic is created as a FIFO topic and whether it uses content-
based
// deduplication instead of ID-based deduplication.
func (actor SnsActions) CreateTopic(topicName string, isFifoTopic bool,
 contentBasedDeduplication bool) (string, error) {
 var topicArn string
 topicAttributes := map[string]string{}
 if isFifoTopic {
  topicAttributes["FifoTopic"] = "true"
 }
 if contentBasedDeduplication {
  topicAttributes["ContentBasedDeduplication"] = "true"
 }
 topic, err := actor.SnsClient.CreateTopic(context.TODO(), &sns.CreateTopicInput{
  Name:       aws.String(topicName),
  Attributes: topicAttributes,
 })
 if err != nil {
  log.Printf("Couldn't create topic %v. Here's why: %v\n", topicName, err)
 } else {
  topicArn = *topic.TopicArn
 }

 return topicArn, err
}
```

- Per i dettagli sull'API, consulta la CreateTopicsezione AWS SDK for Go API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sns.SnsClient;
import software.amazon.awssdk.services.sns.model.CreateTopicRequest;
import software.amazon.awssdk.services.sns.model.CreateTopicResponse;
import software.amazon.awssdk.services.sns.model.SnsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateTopic {
    public static void main(String[] args) {
        final String usage = """

                Usage:    <topicName>

                Where:
                   topicName - The name of the topic to create (for example,
 mytopic).

                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String topicName = args[0];
        System.out.println("Creating a topic with name: " + topicName);
        SnsClient snsClient = SnsClient.builder()
                .region(Region.US_EAST_1)
                .build();

        String arnVal = createSNSTopic(snsClient, topicName);
        System.out.println("The topic ARN is" + arnVal);
        snsClient.close();
    }
```

```
    public static String createSNSTopic(SnsClient snsClient, String topicName) {
        CreateTopicResponse result;
        try {
            CreateTopicRequest request = CreateTopicRequest.builder()
                    .name(topicName)
                    .build();

            result = snsClient.createTopic(request);
            return result.topicArn();

        } catch (SnsException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }
}
```

- Per i dettagli sull'API, consulta la CreateTopicsezione AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Creare il client in un modulo separato ed esportarlo.

```
import { SNSClient } from "@aws-sdk/client-sns";

// The AWS Region can be provided here using the `region` property. If you leave
 it blank
// the SDK will default to the region set in your AWS config.
export const snsClient = new SNSClient({});
```

Importare l'SDK e i moduli client e chiamare l'API.

```
import { CreateTopicCommand } from "@aws-sdk/client-sns";
import { snsClient } from "../libs/snsClient.js";

/**
 * @param {string} topicName - The name of the topic to create.
 */
export const createTopic = async (topicName = "TOPIC_NAME") => {
  const response = await snsClient.send(
    new CreateTopicCommand({ Name: topicName }),
  );
  console.log(response);
  // {
  //   '$metadata': {
  //     httpStatusCode: 200,
  //     requestId: '087b8ad2-4593-50c4-a496-d7e90b82cf3e',
  //     extendedRequestId: undefined,
  //     cfId: undefined,
  //     attempts: 1,
  //     totalRetryDelay: 0
  //   },
  //   TopicArn: 'arn:aws:sns:us-east-1:xxxxxxxxxxxx:TOPIC_NAME'
  // }
  return response;
};
```

- Per ulteriori informazioni, consulta la Guida per sviluppatori di AWS SDK for JavaScript.
- Per i dettagli sull'API, consulta la CreateTopicsezione AWS SDK for JavaScript API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun createSNSTopic(topicName: String): String {
    val request =
        CreateTopicRequest {
            name = topicName
        }

    SnsClient { region = "us-east-1" }.use { snsClient ->
        val result = snsClient.createTopic(request)
        return result.topicArn.toString()
    }
}
```

- Per i dettagli sull'API, CreateTopicconsulta AWS SDK for Kotlin API reference.

PHP

SDK per PHP

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
require 'vendor/autoload.php';

use Aws\Exception\AwsException;
use Aws\Sns\SnsClient;


/**
 * Create a Simple Notification Service topics in your AWS account at the
 requested region.
 *
 * This code expects that you have AWS credentials set up per:
 * https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/
guide_credentials.html
 */

$SnSclient = new SnsClient([
```

```
    'profile' => 'default',
    'region' => 'us-east-1',
    'version' => '2010-03-31'
]);

$topicname = 'myTopic';

try {
    $result = $SnSclient->createTopic([
        'Name' => $topicname,
    ]);
    var_dump($result);
} catch (AwsException $e) {
    // output error message if fails
    error_log($e->getMessage());
}
```

- Per ulteriori informazioni, consulta la Guida per sviluppatori di AWS SDK for PHP.
- Per i dettagli sull'API, consulta la CreateTopicsezione AWS SDK for PHP API Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class SnsWrapper:
    """Encapsulates Amazon SNS topic and subscription functions."""

    def __init__(self, sns_resource):
        """
        :param sns_resource: A Boto3 Amazon SNS resource.
        """
        self.sns_resource = sns_resource
```

```
    def create_topic(self, name):
        """
        Creates a notification topic.

        :param name: The name of the topic to create.
        :return: The newly created topic.
        """
        try:
            topic = self.sns_resource.create_topic(Name=name)
            logger.info("Created topic %s with ARN %s.", name, topic.arn)
        except ClientError:
            logger.exception("Couldn't create topic %s.", name)
            raise
        else:
            return topic
```

- Per i dettagli sull'API, consulta CreateTopic AWSSDK for Python (Boto3) API Reference.

Ruby

SDK per Ruby

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
# This class demonstrates how to create an Amazon Simple Notification Service
 (SNS) topic.
class SNSTopicCreator
  # Initializes an SNS client.
  #
  # Utilizes the default AWS configuration for region and credentials.
  def initialize
    @sns_client = Aws::SNS::Client.new
  end

  # Attempts to create an SNS topic with the specified name.
```

```
  #
  # @param topic_name [String] The name of the SNS topic to create.
  # @return [Boolean] true if the topic was successfully created, false
 otherwise.
  def create_topic(topic_name)
    @sns_client.create_topic(name: topic_name)
    puts "The topic '#{topic_name}' was successfully created."
    true
  rescue Aws::SNS::Errors::ServiceError => e
    # Handles SNS service errors gracefully.
    puts "Error while creating the topic named '#{topic_name}': #{e.message}"
    false
  end
end

# Example usage:
if $PROGRAM_NAME == __FILE__
  topic_name = "YourTopicName" # Replace with your topic name
  sns_topic_creator = SNSTopicCreator.new

  puts "Creating the topic '#{topic_name}'..."
  unless sns_topic_creator.create_topic(topic_name)
    puts "The topic was not created. Stopping program."
    exit 1
  end
end
```

- Per ulteriori informazioni, consulta la Guida per sviluppatori di AWS SDK for Ruby.
- Per i dettagli sull'API, consulta la CreateTopicsezione AWS SDK for Ruby API Reference.

Rust

SDK per Rust

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
async fn make_topic(client: &Client, topic_name: &str) -> Result<(), Error> {
    let resp = client.create_topic().name(topic_name).send().await?;

    println!(
        "Created topic with ARN: {}",
        resp.topic_arn().unwrap_or_default()
    );

    Ok(())
}
```

- Per i dettagli sulle API, consulta la CreateTopicguida di riferimento all'API AWS SDK for Rust.

SAP ABAP

SDK per SAP ABAP

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    TRY.
        oo_result = lo_sns->createtopic( iv_name = iv_topic_name ). " oo_result
 is returned for testing purposes. "
        MESSAGE 'SNS topic created' TYPE 'I'.
      CATCH /aws1/cx_snstopiclimitexcdex.
        MESSAGE 'Unable to create more topics. You have reached the maximum
 number of topics allowed.' TYPE 'E'.
    ENDTRY.
```

- Per i dettagli sulle API, CreateTopicconsulta AWS SDK for SAP ABAP API reference.

> **Note**
>
> Puoi utilizzare anche un argomento Amazon SNS di un altro account, ma in questo caso potrebbe essere necessario creare una policy che conceda all'argomento le autorizzazioni di accesso a AWS Config. Per informazioni sulla concessione di autorizzazioni a un argomento Amazon SNS, consulta Autorizzazioni per l'argomento Amazon SNS e quindi vai a Creazione di un ruolo IAM.

Creazione di un ruolo IAM

Tramite la console IAM

Puoi utilizzare la console IAM per creare un ruolo IAM che conceda AWS Config le autorizzazioni per accedere al tuo bucket Amazon S3, accedere all'argomento Amazon SNS e ottenere dettagli di configurazione per le risorse supportate. AWS Quando utilizzi la console per creare un ruolo IAM, AWS Config collega automaticamente al ruolo le autorizzazioni richieste per tuo conto.

> **Note**
>
> Se hai utilizzato un AWS servizio che utilizza AWS Config (come AWS Security Hub o AWS Control Tower) e un AWS Config ruolo è già stato creato, assicurati che il ruolo IAM che usi durante la configurazione AWS Config mantenga gli stessi privilegi minimi del AWS Config ruolo già creato in modo che l'altro AWS servizio continui a funzionare come previsto.
> Ad esempio, se AWS Control Tower ha un ruolo IAM che AWS Config consente di leggere oggetti Amazon S3, dovresti garantire che vengano concesse le stesse autorizzazioni all'interno del ruolo IAM che usi durante la configurazione. AWS Config Altrimenti, potrebbe interferire con le operazioni di AWS Control Tower.
> Per ulteriori informazioni sui ruoli IAM per AWS Config, consulta AWS Identity and Access Management.

Per creare un ruolo per un AWS servizio

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM, scegliere Ruoli e quindi Crea ruolo.
3. In Seleziona tipo di entità attendibile, scegli Servizio AWS .

4. Scegli il caso d'uso che desideri AWS Config: Config - Customizable, Config - Organizations, Config o Config - Conformance Packs. Quindi, seleziona Next (Successivo).
5. Nella pagina Nomina, verifica e crea, controlla i dettagli del ruolo e seleziona Crea ruolo.

AWS Utilizzo degli SDK

Per utilizzare un AWS SDK, devi configurarlo con le tue credenziali. Per ulteriori informazioni, consulta File di configurazione e credenziali condivisi nella Guida di riferimento per SDK AWS e strumenti.

I seguenti esempi di codice mostrano come utilizzare. `CreateRole`

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro da fare GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// Create a new IAM role.
    /// </summary>
    /// <param name="roleName">The name of the IAM role.</param>
    /// <param name="rolePolicyDocument">The name of the IAM policy document
    /// for the new role.</param>
    /// <returns>The Amazon Resource Name (ARN) of the role.</returns>
    public async Task<string> CreateRoleAsync(string roleName, string
rolePolicyDocument)
    {
        var request = new CreateRoleRequest
        {
            RoleName = roleName,
            AssumeRolePolicyDocument = rolePolicyDocument,
        };

        var response = await _IAMService.CreateRoleAsync(request);
        return response.Role.Arn;
    }
```

- Per i dettagli sull'API, consulta la CreateRolesezione AWS SDK for .NET API Reference.

Bash

AWS CLI con lo script Bash

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_create_role
#
# This function creates an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
#       The ARN of the role.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_role() {
  local role_name policy_document response
  local option OPTARG # Required to use getopts command in a function.
```

```
# bashsupport disable=BP5008
function usage() {
  echo "function iam_create_user_access_key"
  echo "Creates an AWS Identity and Access Management (IAM) role."
  echo "  -n role_name   The name of the IAM role."
  echo "  -p policy_json -- The assume role policy document."
  echo ""
}

# Retrieve the calling parameters.
while getopts "n:p:h" option; do
  case "${option}" in
    n) role_name="${OPTARG}" ;;
    p) policy_document="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$role_name" ]]; then
  errecho "ERROR: You must provide a role name with the -n parameter."
  usage
  return 1
fi

if [[ -z "$policy_document" ]]; then
  errecho "ERROR: You must provide a policy document with the -p parameter."
  usage
  return 1
fi

response=$(aws iam create-role \
  --role-name "$role_name" \
  --assume-role-policy-document "$policy_document" \
  --output text \
```

```
    --query Role.Arn)

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Per i dettagli sull'API, consulta CreateRole AWS CLICommand Reference.

C++

SDK per C++

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
bool AwsDoc::IAM::createIamRole(
        const Aws::String &roleName,
        const Aws::String &policy,
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::IAM::IAMClient client(clientConfig);
    Aws::IAM::Model::CreateRoleRequest request;

    request.SetRoleName(roleName);
    request.SetAssumeRolePolicyDocument(policy);

    Aws::IAM::Model::CreateRoleOutcome outcome = client.CreateRole(request);
    if (!outcome.IsSuccess()) {
        std::cerr << "Error creating role. " <<
                  outcome.GetError().GetMessage() << std::endl;
```

```
    }
    else {
        const Aws::IAM::Model::Role iamRole = outcome.GetResult().GetRole();
        std::cout << "Created role " << iamRole.GetRoleName() << "\n";
        std::cout << "ID: " << iamRole.GetRoleId() << "\n";
        std::cout << "ARN: " << iamRole.GetArn() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Per i dettagli sull'API, consulta la CreateRolesezione AWS SDK for C++ API Reference.

CLI

AWS CLI

Esempio 1: Come creare un ruolo IAM

Il comando `create-role` seguente crea un ruolo denominato `Test-Role` e collega una policy di attendibilità a tale ruolo.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json
```

Output:

```
{
    "Role": {
        "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2013-06-07T20:43:32.821Z",
        "RoleName": "Test-Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

La policy di attendibilità è definita come documento JSON nel file Test-Role-Trust-Policy.json. (Il nome e l'estensione del file non hanno importanza.) La policy di attendibilità deve specificare un principale.

Per collegare una policy di autorizzazioni a un ruolo, usa il comando `put-role-policy`.

Per ulteriori informazioni, consulta Creazione di ruoli IAM nella Guida per l'utente IAM AWS .

Esempio 2: Come creare un ruolo IAM con una durata massima della sessione specificata

Il comando `create-role` seguente crea un ruolo denominato `Test-Role` e imposta una durata massima della sessione di 7200 secondi (2 ore).

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --max-session-duration 7200
```

Output:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:role/Test-Role",
        "CreateDate": "2023-05-24T23:50:25+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::12345678012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Per ulteriori informazioni, consulta Modificare la durata massima della sessione (AWS API) di un ruolo nella Guida per l'utente AWS IAM.

Esempio 3: Come creare un ruolo IAM con tag

Il comando seguente crea un ruolo IAM `Test-Role` con tag. Questo esempio utilizza il flag del parametro `--tags` con i seguenti tag in formato JSON: `'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`. In alternativa, il flag `--tags` può essere utilizzato con tag in formato abbreviato: `'Key=Department,Value=Accounting Key=Location,Value=Seattle'`.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

Output:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "Tags": [
            {
                "Key": "Department",
```

```
                "Value": "Accounting"
            },
            {
                "Key": "Location",
                "Value": "Seattle"
            }
        ]
    }
}
```

Per ulteriori informazioni, consulta Applicazione di tag a ruoli IAM nella Guida per l'utente di IAM AWS .

- Per i dettagli sull'API, consulta CreateRole AWS CLICommand Reference.

Go

SDK per Go V2

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
// RoleWrapper encapsulates AWS Identity and Access Management (IAM) role actions
// used in the examples.
// It contains an IAM service client that is used to perform role actions.
type RoleWrapper struct {
 IamClient *iam.Client
}



// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
// serialize it to JSON by using Go's JSON marshaler.
```

```
func (wrapper RoleWrapper) CreateRole(roleName string, trustedUserArn string)
 (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version:   "2012-10-17",
  Statement: []PolicyStatement{{
   Effect: "Allow",
   Principal: map[string]string{"AWS": trustedUserArn},
   Action: []string{"sts:AssumeRole"},
  }},
 }
 policyBytes, err := json.Marshal(trustPolicy)
 if err != nil {
  log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
 trustedUserArn, err)
  return nil, err
 }
 result, err := wrapper.IamClient.CreateRole(context.TODO(),
 &iam.CreateRoleInput{
  AssumeRolePolicyDocument: aws.String(string(policyBytes)),
  RoleName:                 aws.String(roleName),
 })
 if err != nil {
  log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
 } else {
  role = result.Role
 }
 return role, err
}
```

- Per i dettagli sull'API, consulta la CreateRolesezione AWS SDK for Go API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import org.json.simple.JSONObject;
import org.json.simple.parser.JSONParser;
import software.amazon.awssdk.services.iam.model.CreateRoleRequest;
import software.amazon.awssdk.services.iam.model.CreateRoleResponse;
import software.amazon.awssdk.services.iam.model.IamException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iam.IamClient;
import java.io.FileReader;

/*
*   This example requires a trust policy document. For more information, see:
*   https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-
roles/
*
*
*  In addition, set up your development environment, including your credentials.
*
*  For information, see this documentation topic:
*
*  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateRole {
    public static void main(String[] args) throws Exception {
        final String usage = """
                Usage:
                    <rolename> <fileLocation>\s

                Where:
                    rolename - The name of the role to create.\s
                    fileLocation - The location of the JSON document that
 represents the trust policy.\s
                """;

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String rolename = args[0];
        String fileLocation = args[1];
        Region region = Region.AWS_GLOBAL;
```

```
        IamClient iam = IamClient.builder()
                .region(region)
                .build();

        String result = createIAMRole(iam, rolename, fileLocation);
        System.out.println("Successfully created user: " + result);
        iam.close();
    }

    public static String createIAMRole(IamClient iam, String rolename, String
 fileLocation) throws Exception {
        try {
            JSONObject jsonObject = (JSONObject)
 readJsonSimpleDemo(fileLocation);
            CreateRoleRequest request = CreateRoleRequest.builder()
                    .roleName(rolename)
                    .assumeRolePolicyDocument(jsonObject.toJSONString())
                    .description("Created using the AWS SDK for Java")
                    .build();

            CreateRoleResponse response = iam.createRole(request);
            System.out.println("The ARN of the role is " +
 response.role().arn());

        } catch (IamException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }

    public static Object readJsonSimpleDemo(String filename) throws Exception {
        FileReader reader = new FileReader(filename);
        JSONParser jsonParser = new JSONParser();
        return jsonParser.parse(reader);
    }
}
```

- Per i dettagli sull'API, consulta la CreateRolesezione AWS SDK for Java 2.x API Reference.

JavaScript

SDK per JavaScript (v3)

> **Note**
>
> C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Crea il ruolo.

```
import { CreateRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const createRole = (roleName) => {
  const command = new CreateRoleCommand({
    AssumeRolePolicyDocument: JSON.stringify({
      Version: "2012-10-17",
      Statement: [
        {
          Effect: "Allow",
          Principal: {
            Service: "lambda.amazonaws.com",
          },
          Action: "sts:AssumeRole",
        },
      ],
    }),
    RoleName: roleName,
  });

  return client.send(command);
};
```

- Per i dettagli sull'API, consulta la CreateRolesezione AWS SDK for JavaScript API Reference.

PHP

SDK per PHP

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
$uuid = uniqid();
$service = new IAMService();

$assumeRolePolicyDocument = "{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Principal\": {\"AWS\": \"{$user['Arn']}\"},
                    \"Action\": \"sts:AssumeRole\"
                }]
            }";
$assumeRoleRole = $service->createRole("iam_demo_role_$uuid",
 $assumeRolePolicyDocument);
echo "Created role: {$assumeRoleRole['RoleName']}\n";

    /**
     * @param string $roleName
     * @param string $rolePolicyDocument
     * @return array
     * @throws AwsException
     */
    public function createRole(string $roleName, string $rolePolicyDocument)
    {
        $result = $this->customWaiter(function () use ($roleName,
 $rolePolicyDocument) {
            return $this->iamClient->createRole([
                'AssumeRolePolicyDocument' => $rolePolicyDocument,
                'RoleName' => $roleName,
```

```
            ]);
        });
        return $result['Role'];
    }
```

- Per i dettagli sull'API, consulta la CreateRolesezione AWS SDK for PHP API Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: Questo esempio crea un nuovo ruolo denominato **MyNewRole** e gli allega la politica trovata nel file**NewRoleTrustPolicy.json**. Si noti che è necessario utilizzare il parametro **-Raw** switch per elaborare correttamente il file di policy JSON. Il documento di policy visualizzato nell'output è codificato in URL. In questo esempio viene decodificato con il **UrlDecode** metodo.NET.

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

Output:

```
Arn                      : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                           %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                           %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                           %20%5D%0D%0A%7D
CreateDate               : 4/15/2015 11:04:23 AM
Path                     : /
RoleId                   : V5PAJI2KPN4EAEXAMPLE1
```

```
RoleName                  : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- Per i dettagli sull'API, vedere CreateRolein AWS Tools for PowerShell Cmdlet Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
def create_role(role_name, allowed_services):
    """
    Creates a role that lets a list of specified services assume the role.

    :param role_name: The name of the role.
    :param allowed_services: The services that can assume the role.
    :return: The newly created role.
    """
    trust_policy = {
        "Version": "2012-10-17",
        "Statement": [
            {
```

```
                "Effect": "Allow",
                "Principal": {"Service": service},
                "Action": "sts:AssumeRole",
            }
            for service in allowed_services
        ],
    }

    try:
        role = iam.create_role(
            RoleName=role_name, AssumeRolePolicyDocument=json.dumps(trust_policy)
        )
        logger.info("Created role %s.", role.name)
    except ClientError:
        logger.exception("Couldn't create role %s.", role_name)
        raise
    else:
        return role
```

- Per i dettagli sull'API, consulta CreateRole AWSSDK for Python (Boto3) API Reference.

Ruby

SDK per Ruby

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
 # Creates a role and attaches policies to it.
 #
 # @param role_name [String] The name of the role.
 # @param assume_role_policy_document [Hash] The trust relationship policy
document.
 # @param policy_arns [Array<String>] The ARNs of the policies to attach.
 # @return [String, nil] The ARN of the new role if successful, or nil if an
error occurred.
```

```
  def create_role(role_name, assume_role_policy_document, policy_arns)
    response = @iam_client.create_role(
      role_name: role_name,
      assume_role_policy_document: assume_role_policy_document.to_json
    )
    role_arn = response.role.arn

    policy_arns.each do |policy_arn|
      @iam_client.attach_role_policy(
        role_name: role_name,
        policy_arn: policy_arn
      )
    end

    role_arn
  rescue Aws::IAM::Errors::ServiceError => e
    @logger.error("Error creating role: #{e.message}")
    nil
  end
```

- Per i dettagli sull'API, consulta la CreateRolesezione AWS SDK for Ruby API Reference.

Rust

SDK per Rust

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
pub async fn create_role(
    client: &iamClient,
    role_name: &str,
    role_policy_document: &str,
) -> Result<Role, iamError> {
    let response: CreateRoleOutput = loop {
        if let Ok(response) = client
            .create_role()
            .role_name(role_name)
```

```
            .assume_role_policy_document(role_policy_document)
            .send()
            .await
        {
            break response;
        }
    };

    Ok(response.role.unwrap())
}
```

- Per i dettagli sulle API, consulta la CreateRoleguida di riferimento all'API AWS SDK for Rust.

Swift

SDK per Swift

> **Note**
>
> Si tratta di una documentazione di pre-rilascio di un SDK nella versione di anteprima. ed è soggetta a modifiche.

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public func createRole(name: String, policyDocument: String) async throws ->
String {
       let input = CreateRoleInput(
           assumeRolePolicyDocument: policyDocument,
           roleName: name
       )
       do {
           let output = try await client.createRole(input: input)
           guard let role = output.role else {
               throw ServiceHandlerError.noSuchRole
```

```
            }
            guard let id = role.roleId else {
                throw ServiceHandlerError.noSuchRole
            }
            return id
        } catch {
            throw error
        }
    }
```

- Per i dettagli sull'API, consulta la CreateRoleguida di riferimento all'API AWS SDK for Swift.

A partire da AWS ConfigAWS CLI

> **Note**
>
> Prima di eseguire la configurazione AWS Config con AWS CLI, devi creare un bucket S3, un argomento SNS e un ruolo IAM con policy allegate come prerequisiti. È quindi possibile utilizzare il AWS CLI per specificare il bucket, l'argomento e il ruolo per. AWS ConfigPer impostare i prerequisiti per AWS Config, consulta Prerequisiti.

Per iniziare AWS CLI, utilizzate AWS Config i comandi put-configuration-recorder, put-delivery-channel e start-configuration-recorder, come segue:

- Il comando `put-configuration-recorder` crea un nuovo registratore di configurazione per registrare le configurazioni delle risorse specificate.
- Il comando `put-delivery-channel` crea un oggetto del canale di distribuzione per distribuire le informazioni di configurazione a un bucket S3 e a un argomento SNS.
- Dopo aver creato un canale di distribuzione, `start-configuration-recorder` inizia a registrare le configurazioni delle risorse selezionate, che puoi vedere nell'account AWS .

> **Note**
>
> Può essere presente un solo registratore di configurazione e un solo canale di distribuzione per ciascuna regione AWS dell'account.

Puoi specificare il nome del registratore e l'Amazon Resource Name (ARN) del ruolo IAM assunto e utilizzato AWS Config dal registratore di configurazione. AWS Config assegna automaticamente il nome «default» durante la creazione del registratore di configurazione. Non puoi modificare il nome del registratore di configurazione una volta creato. Per modificare il nome del registratore della configurazione, devi eliminarlo e creare un nuovo registratore della configurazione con un nuovo nome.

AWS Config Per configurare l'aggregazione di dati multiregione con più account con AWS CLI, consulta Configurazione di un aggregatore tramite l'interfaccia a riga di comando. AWS È necessario creare un registratore di configurazione separato per ogni regione in Account AWS cui si desidera registrare gli elementi di configurazione.

Indice

- put-configuration-recorder
- put-delivery-channel
- start-configuration-recorder

put-configuration-recorder

Il comando `put-configuration-recorder` deve assomigliare a quello riportato nell'esempio seguente.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

Questo comando utilizza i `---recording-group` campi `--configuration-recorder` and.

> **Note**
>
> Gruppo di registrazione e registratore di configurazione
>
> Il campo `--recording-group` specifica quali tipi di risorse vengono registrati.
>
> Il `--configuration-recorder` campo specifica `name` e la frequenza `roleArn` di registrazione predefinita per il registratore di configurazione (). `recordingMode` È inoltre possibile utilizzare questo campo per sovrascrivere la frequenza di registrazione per tipi di risorse specifici.

Gruppo di registrazione

`put-configuration-recorder` usa le seguenti opzioni per il parametro `--recording-group`:

- `allSupported=true`— AWS Config registra le modifiche alla configurazione per tutti i tipi di risorse supportati, esclusi i tipi di risorse IAM globali. Quando AWS Config aggiunge il supporto per un nuovo tipo di risorsa, avvia AWS Config automaticamente la registrazione delle risorse di quel tipo.
- `includeGlobalResourceTypes=true`: questa opzione è un bundle che si applica solo ai tipi di risorse IAM registrati a livello globale: utenti IAM, gruppi, ruoli e policy gestite dal cliente. Questi tipi di risorse IAM globali possono essere registrati solo AWS Config nelle regioni in cui AWS Config erano disponibili prima di febbraio 2022. Non è possibile registrare i tipi di risorse IAM globali nelle regioni supportate AWS Config entro febbraio 2022. Per un elenco di tali regioni, consulta Risorse di registrazione | AWS Risorse globali.

> **Important**
>
> I cluster globali Aurora sono registrati in tutte le regioni abilitate
> Il tipo di `AWS::RDS::GlobalCluster` risorsa verrà registrato in tutte le AWS Config regioni supportate in cui il registratore di configurazione è abilitato, anche se `includeGlobalResourceTypes` è impostato `false` su. L'opzione `includeGlobalResourceTypes` è un pacchetto applicabile solo agli utenti IAM, ai gruppi, ai ruoli e alle policy gestite dal cliente.
> Se non desideri registrare `AWS::RDS::GlobalCluster` in tutte le regioni abilitate, utilizza una delle seguenti strategie di registrazione:
>
> 1. Registra tutti i tipi di risorse attuali e futuri con esclusioni (`EXCLUSION_BY_RESOURCE_TYPES`) oppure
> 2. Registra tipi di risorsa specifici (`INCLUSION_BY_RESOURCE_TYPES`).
>
> Per ulteriori informazioni, consulta Scegli quali risorse devono essere registrate.

> **Important**
>
> strategia di GlobalResourceTypes registrazione di inclusione ed esclusione
> Il `includeGlobalResourceTypes` campo non ha alcun impatto sulla strategia `EXCLUSION_BY_RESOURCE_TYPES` di registrazione. Ciò significa che i tipi di risorse IAM globali (utenti IAM, gruppi, ruoli e policy gestite dai clienti) non verranno aggiunti

automaticamente come esclusioni per `exclusionByResourceTypes` quando `includeGlobalResourceTypes` è impostato su. `false`
Il `includeGlobalResourceTypes` campo deve essere utilizzato solo per modificare il `AllSupported` campo, poiché l'impostazione predefinita per il `AllSupported` campo consiste nel registrare le modifiche alla configurazione per tutti i tipi di risorse supportati, esclusi i tipi di risorse IAM globali. Per includere i tipi di risorse IAM globali quando `AllSupported` è impostato su`true`, assicurati di `includeGlobalResourceTypes` impostarlo su`true`.
Per escludere i tipi di risorse IAM globali per la strategia di `EXCLUSION_BY_RESOURCE_TYPES` registrazione, devi aggiungerli manualmente al `resourceTypes` campo di`exclusionByResourceTypes`.

> **Note**
>
> Campi obbligatori e facoltativi
> Prima di impostare `includeGlobalResourceTypes` su `true`, imposta il campo `allSupported` su `true`.
> Facoltativamente, puoi anche impostare il campo `useOnly` di `RecordingStrategy` su `ALL_SUPPORTED_RESOURCE_TYPES`.

> **Note**
>
> Sostituzione dei campi
> Se `includeGlobalResourceTypes` imposti su `false` ma elenchi i tipi di risorse IAM globali nel `resourceTypes` campo di RecordingGroup, AWS Config registrerà comunque le modifiche alla configurazione per quei tipi di risorse specificati indipendentemente dal fatto che il `includeGlobalResourceTypes` campo sia impostato su false.
> Se non desideri registrare le modifiche alla configurazione dei tipi di risorse IAM registrati a livello globale (policy gestite dal cliente o da gruppi, ruoli e utenti IAM), assicurati di non elencarli nel campo `resourceTypes` e di impostare il campo `includeGlobalResourceTypes` su false.

- `recordingStrategy`: specifica la strategia di registrazione per il registratore di configurazione. Il file `recordingGroup.json` specifica quali tipi di risorse saranno registrate da AWS Config :

- Se imposti il `useOnly` campo su`ALL_SUPPORTED_RESOURCE_TYPES`, AWS Config registra le modifiche RecordingStrategyalla configurazione per tutti i tipi di risorse supportati, esclusi i tipi di risorse IAM globali. Facoltativamente, puoi impostare il `allSupported` campo RecordingGroupsu`true`. Quando AWS Config aggiunge il supporto per un nuovo tipo di risorsa, avvia AWS Config automaticamente la registrazione delle risorse di quel tipo.
- Se si imposta il `useOnly` campo su`INCLUSION_BY_RESOURCE_TYPES`, AWS Config registra le modifiche RecordingStrategyalla configurazione solo per i tipi di risorse specificati nel `resourceTypes` campo di RecordingGroup.
- Se si imposta il `useOnly` campo su`EXCLUSION_BY_RESOURCE_TYPES`, AWS Config registra le modifiche RecordingStrategyalla configurazione per tutti i tipi di risorse supportati ad eccezione dei tipi di risorse che si specifica di escludere dalla registrazione nel `resourceTypes` campo di ExclusionByResourceTypes.

> **Note**
>
> Campi obbligatori e facoltativi
>
> Il campo `recordingStrategy` è facoltativo se imposti il campo `allSupported` di `--recording-group` su `true`.
>
> Il campo `recordingStrategy` è facoltativo se elenchi i tipi di risorse nel campo `resourceTypes` di `--recording-group`.
>
> Il campo `recordingStrategy` è obbligatorio se elenchi i tipi di risorse da escludere dalla registrazione nel campo `resourceTypes` di `exclusionByResourceTypes`.

> **Note**
>
> Sostituzione dei campi
>
> Se scegli `EXCLUSION_BY_RESOURCE_TYPES` come strategia di registrazione, il campo `exclusionByResourceTypes` sovrascrive le altre proprietà della richiesta.
>
> Ad esempio, anche se hai impostato `includeGlobalResourceTypes` su false, i tipi di risorse IAM registrati a livello globale verranno comunque registrati automaticamente in questa opzione, a meno che tali tipi di risorse non siano specificamente elencati come esenzioni nel campo `resourceTypes` di `exclusionByResourceTypes`.

> **Note**
>
> Tipi di risorse globali e strategia di registrazione di esclusione delle risorse
> Per impostazione predefinita, se si sceglie la strategia di `EXCLUSION_BY_RESOURCE_TYPES` registrazione, When AWS Config aggiunge il supporto per un nuovo tipo di risorsa nella regione in cui è impostato il registratore di configurazione, inclusi i tipi di risorse globali, AWS Config avvia automaticamente la registrazione delle risorse di quel tipo.
> A meno che non siano specificatamente elencate come esclusioni, `AWS::RDS::GlobalCluster` verranno registrate automaticamente in tutte le AWS Config regioni supportate in cui il registratore di configurazione è abilitato.
> Gli utenti, i gruppi, i ruoli e le politiche gestite dai clienti di IAM verranno registrati nella regione in cui è stato configurato il registratore di configurazione, se questa è una regione in cui AWS Config era disponibile prima di febbraio 2022. Non puoi registrare i tipi di risorse IAM globali nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta Risorse di registrazione | AWS Risorse globali.

Di seguito è riportata la sintassi della richiesta per `recordingGroup.json`.

```
{
    "allSupported": boolean,
    "exclusionByResourceTypes": {
        "resourceTypes": [ Comma-separated list of resource types to exclude ]
    },
    "includeGlobalResourceTypes": boolean,
    "recordingStrategy": {
        "useOnly": "Recording strategy for the configuration recorder"
    },
    "resourceTypes": [ Comma-separated list of resource types to include]
}
```

> **Note**
>
> Politiche di autorizzazione per AWS Organizations Can Prevent Access
> Se utilizzi un ruolo IAM preesistente, assicurati che non esista una politica di autorizzazione AWS Organizations che AWS Config impedisca di avere il permesso di registrare le tue

risorse. Per ulteriori informazioni sulle politiche di autorizzazione per AWS Organizations, consulta la sezione Gestione delle politiche AWS Organizations nella Guida per l'AWS Organizations utente.

Mantieni le autorizzazioni minime quando riutilizzi un ruolo IAM

Se utilizzi un AWS servizio che utilizza AWS Config, come AWS Security Hub o AWS Control Tower, e un ruolo IAM è già stato creato, assicurati che il ruolo IAM che usi durante la configurazione AWS Config mantenga le stesse autorizzazioni minime del ruolo IAM preesistente. È necessario eseguire questa operazione per garantire che l'altro AWS servizio continui a funzionare come previsto.

Ad esempio, se AWS Control Tower dispone di un ruolo IAM che AWS Config consente di leggere oggetti S3, assicurati che vengano concesse le stesse autorizzazioni al ruolo IAM che utilizzi durante la configurazione. AWS Config Altrimenti, potrebbe interferire con il funzionamento AWS Control Tower .

Note

Numero elevato di AWS Config valutazioni

Potresti notare una maggiore attività nel tuo account durante la registrazione del mese iniziale con AWS Config rispetto ai mesi successivi. Durante il processo di avvio iniziale, AWS Config esegue valutazioni su tutte le risorse dell'account che hai selezionato per la AWS Config registrazione.

Se esegui carichi di lavoro temporanei, potresti riscontrare un aumento dell'attività dovuto alla registrazione delle modifiche alla configurazione associate alla creazione e all'eliminazione di queste risorse temporanee. AWS Config Un carico di lavoro temporaneo è un uso temporaneo di risorse di elaborazione che vengono caricate ed eseguite quando necessario. Gli esempi includono istanze Spot Amazon Elastic Compute Cloud (Amazon EC2), lavori Amazon EMR e. AWS Auto Scaling Se vuoi evitare l'aumento dell'attività dovuto all'esecuzione di carichi di lavoro temporanei, puoi configurare il registratore di configurazione per escludere questi tipi di risorse dalla registrazione o eseguire questi tipi di carichi di lavoro in un account separato con AWS Config disattivato per evitare un aumento della registrazione della configurazione e delle valutazioni delle regole.

> **Note**
>
> Disponibilità nelle regioni
>
> Prima di specificare un tipo di risorsa da AWS Config monitorare, controllate la disponibilità della copertura delle risorse per regione per verificare se il tipo di risorsa è supportato nella regione in cui state effettuando la AWS configurazione. AWS Config Se un tipo di risorsa è supportato da AWS Config almeno una regione, puoi abilitare la registrazione di quel tipo di risorsa in tutte le regioni supportate da AWS Config, anche se il tipo di risorsa specificato non è supportato nella AWS regione in cui stai effettuando la configurazione AWS Config.

Registratore della configurazione di

`put-configuration-recorder` usa i seguenti campi per il parametro `--configuration-recorder`:

- `name`— Il nome del registratore di configurazione. AWS Config assegna automaticamente il nome di «default» durante la creazione del registratore di configurazione.
- `roleARN`— Amazon Resource Name (ARN) del ruolo IAM assunto AWS Config e utilizzato dal registratore di configurazione.
- `recordingMode`— Speciifica la frequenza di registrazione predefinita AWS Config utilizzata per registrare le modifiche alla configurazione. AWS Config supporta la registrazione continua e la registrazione giornaliera. La registrazione continua consente di registrare continuamente le modifiche alla configurazione ogni volta che si verifica una modifica. La registrazione giornaliera consente di ricevere un elemento di configurazione (CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza.
  - `recordingFrequency`— La frequenza di registrazione predefinita AWS Config utilizzata per registrare le modifiche alla configurazione.

> **Note**
>
> AWS Firewall Manager dipende dalla registrazione continua per monitorare le risorse. Se si utilizza Firewall Manager, si consiglia di impostare la frequenza di registrazione su Continuo.

- `recordingModeOverrides`: questo campo consente di specificare le sostituzioni per la modalità di registrazione. Si tratta di un array di oggetti `recordingModeOverride`. Ogni oggetto `recordingModeOverride` dell'array `recordingModeOverrides` è composto da tre campi:
  - `description`— Una descrizione fornita per l'override.
  - `recordingFrequency`— La frequenza di registrazione che verrà applicata a tutti i tipi di risorse specificati nell'override.
  - `resourceTypes`— Un elenco separato da virgole che specifica quali tipi di risorse sono AWS Config inclusi nell'override.

> **Note**
>
> Campi obbligatori e facoltativi
>
> Il campo `recordingMode` per `put-configuration-recorder` è facoltativo. Per impostazione predefinita, la frequenza di registrazione per il registratore di configurazione è impostata su Registrazione continua.

> **Note**
>
> Limiti
>
> La registrazione giornaliera non è supportata per i tipi di risorse seguenti:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> Per la strategia di registrazione Registra tutti i tipi di risorse supportati attuali e futuri (`ALL_SUPPORTED_RESOURCE_TYPES`), questi tipi di risorse saranno impostati su Registrazione continua.

Il `configurationRecorder.json` file specifica `name` e `roleArn` la frequenza di registrazione predefinita per il registratore di configurazione (). `recordingMode` È inoltre possibile utilizzare questo campo per sovrascrivere la frequenza di registrazione per tipi di risorse specifici.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in the
 override ]
        }
    ]
  }
}
```

put-delivery-channel

I seguenti esempi di codice mostrano come utilizzare. `PutDeliveryChannel`

CLI

AWS CLI

Per creare un canale di distribuzione

Il comando seguente fornisce le impostazioni per il canale di consegna come codice JSON:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

Il `deliveryChannel.json` file specifica gli attributi del canale di consegna:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

L'esempio seguente imposta i seguenti attributi:

`name`- Il nome del canale di consegna. Per impostazione predefinita, AWS Config assegna il nome `default` a un nuovo canale di consegna. Non è possibile aggiornare il nome del canale di consegna con il comando. `put-delivery-channel` Per i passaggi per modificare il nome, vedi Ridenominazione del canale di consegna. `s3BucketName` - Il nome del bucket Amazon S3 a cui AWS Config fornisce istantanee di configurazione e file di cronologia della configurazione. Se si specifica un bucket che appartiene a un altro AWS account, tale bucket deve disporre di politiche che concedano le autorizzazioni di accesso a Config. AWS Per ulteriori informazioni, consulta Autorizzazioni per il bucket Amazon S3.

`snsTopicARN`- L'Amazon Resource Name (ARN) dell'argomento Amazon SNS a cui AWS Config invia notifiche sulle modifiche alla configurazione. Se scegli un argomento da un altro account, l'argomento deve avere politiche che concedano le autorizzazioni di accesso a Config. AWS Per ulteriori informazioni, consulta l'argomento Autorizzazioni per l'argomento Amazon SNS.

`configSnapshotDeliveryProperties`- Contiene l'`deliveryFrequency`attributo, che imposta la frequenza con cui AWS Config fornisce istantanee di configurazione e la frequenza con cui richiama le valutazioni per le regole Config periodiche.

Se il comando ha esito positivo, AWS Config non restituisce alcun output. Per verificare le impostazioni del tuo canale di consegna, esegui il describe-delivery-channels comando.

- Per i dettagli sull'API, consulta PutDeliveryChannel in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio modifica la proprietà DeliveryFrequency di un canale di consegna esistente.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- Per i dettagli sull'API, vedere PutDeliveryChannel in AWS Tools for PowerShell Cmdlet Reference.

start-configuration-recorder

Per terminare l'accensione AWS Config, utilizzare il `start-configuration-recorder`comando.

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Verifica che AWS Config sia stata avviata correttamente con il AWS CLI

Dopo l'avvio AWS Config, è possibile utilizzare AWS CLI i comandi per verificare che AWS Config sia in esecuzione e che siano AWS Config stati creati un registratore di configurazione e un canale di distribuzione. È inoltre possibile confermare di aver AWS Config avviato la registrazione e l'invio delle configurazioni al canale di distribuzione.

Indice

- Verifica della creazione del canale di distribuzione
- Verifica della creazione del registratore di configurazione
- Verifica che la registrazione sia iniziata AWS Config

Verifica della creazione del canale di distribuzione

Utilizza il comando `describe-delivery-channels` per verificare che il bucket Amazon S3 e l'argomento Amazon SNS siano stati configurati.

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
            "name": "my-delivery-channel",
            "s3BucketName": "my-config-bucket"
        }
    ]
}
```

Quando utilizzi la CLI, l'API del servizio o gli SDK per configurare il tuo canale di distribuzione e non specifichi un nome, assegna AWS Config automaticamente il nome "». `default`

Verifica della creazione del registratore di configurazione

Utilizza il comando `describe-configuration-recorders` per verificare che un registratore di configurazione sia stato creato e che abbia assunto un ruolo IAM. Per ulteriori informazioni, consulta Creazione di un ruolo IAM.

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

Verifica che la registrazione sia iniziata AWS Config

Usa il `describe-configuration-recorder-status`comando per verificare che AWS Config abbia iniziato a registrare le configurazioni delle AWS risorse supportate esistenti nel tuo account. Le configurazioni registrate vengono consegnate al canale di distribuzione specificato.

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

Il valore `true` del campo `recording` conferma che il registratore di configurazione ha iniziato a registrare le configurazioni di tutte le risorse. AWS Config registra l'ora in formato UTC. L'output viene visualizzato come timestamp Unix.

Per ulteriori informazioni su come cercare le risorse esistenti nel tuo account e comprendere le configurazioni delle risorse, vedere Visualizzazione delle configurazioni e della cronologia delle risorse di .

Utilizzo AWS Config con un SDK AWS

AWS I kit di sviluppo software (SDK) sono disponibili per molti linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice, e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.

Documentazione sugli SDK	Esempi di codice
AWS SDK for C++	AWS SDK for C++ esempi di codice
AWS CLI	AWS CLI esempi di codice
AWS SDK for Go	AWS SDK for Go esempi di codice
AWS SDK for Java	AWS SDK for Java esempi di codice
AWS SDK for JavaScript	AWS SDK for JavaScript esempi di codice
SDK AWS for Kotlin	SDK AWS for Kotlin esempi di codice
AWS SDK for .NET	AWS SDK for .NET esempi di codice
AWS SDK for PHP	AWS SDK for PHP esempi di codice
AWS Tools for PowerShell	Strumenti per esempi di PowerShell codice
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) esempi di codice
AWS SDK for Ruby	AWS SDK for Ruby esempi di codice
AWS SDK for Rust	AWS SDK for Rust esempi di codice
SDK AWS per SAP ABAP	SDK AWS per SAP ABAP esempi di codice
SDK AWS per Swift	SDK AWS per Swift esempi di codice

Esempio di disponibilità

Non riesci a trovare quello che ti serve? Richiedi un esempio di codice utilizzando il link Provide feedback (Fornisci un feedback) nella parte inferiore di questa pagina.

Gestione del registratore della configurazione

AWS Config utilizza il registratore di configurazione per rilevare le modifiche nelle configurazioni delle risorse e acquisire tali modifiche come elementi di configurazione. È necessario creare un registratore di configurazione prima di AWS Config poter tenere traccia delle configurazioni delle risorse. Quando avvii il registratore di configurazione, AWS Config fa un inventario di tutte le AWS risorse del tuo account.

È possibile disporre di un solo canale di registrazione per AWS regione e Account AWS il canale di distribuzione è necessario utilizzare. AWS Config

Se si esegue la configurazione AWS Config utilizzando la console o la AWS CLI, crea AWS Config automaticamente e quindi avvia automaticamente il registratore di configurazione. Per ulteriori informazioni, consulta Guida introduttiva con AWS Config.

Per impostazione predefinita, il registratore della configurazione registra tutte le risorse supportate nella regione in cui AWS Config è in esecuzione. Puoi creare un registratore della configurazione personalizzato che registra solo i tipi di risorse specificati dall'utente. Per ulteriori informazioni, consulta AWS Risorse per la registrazione.

All' AWS Config inizio della registrazione delle configurazioni ti vengono addebitati i costi di utilizzo del servizio. Per informazioni sui prezzi, consulta Prezzi di AWS Config.

> **Important**
>
> I risultati della valutazione per le risorse eliminate possono persistere se il Configuration Recorder non è attivo
> Se il registratore di configurazione è spento, disabilita la capacità di tenere traccia delle modifiche AWS Config alla configurazione delle risorse, incluse le relative eliminazioni. Ciò significa che potresti vedere i risultati della valutazione per le risorse che sono state precedentemente eliminate se disattivi il registratore di configurazione.

Gestione del registratore della configurazione (Console)

È possibile utilizzare la AWS Config console per arrestare o avviare il registratore di configurazione. È inoltre possibile modificare la frequenza di registrazione del registratore di configurazione.

To stop or start the configuration recorder

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Scegliere Settings (Impostazioni) nel riquadro di navigazione.
3. Arresta o avvia il registratore della configurazione:
   - Se desideri interrompere la registrazione, in La registrazione è attivata, scegli Disattiva. Quando richiesto, scegli Continua.
   - Se desideri avviare la registrazione, in La registrazione è disattivata, scegli Attiva. Quando richiesto, scegli Continua.

To change the recording frequency

AWS Config supporta la registrazione continua e la registrazione giornaliera. La registrazione continua consente di registrare continuamente le modifiche alla configurazione ogni volta che si verifica una modifica. La registrazione giornaliera consente di ricevere un elemento di configurazione (CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza. Per ulteriori informazioni, vedere Frequenza di registrazione.

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Scegliere Settings (Impostazioni) nel riquadro di navigazione.
3. Scegli Modifica per visualizzare le opzioni in “Frequenza di registrazione”.

Gestione del registratore della configurazione (AWS CLI)

È possibile utilizzare il AWS CLI per arrestare o avviare il registratore di configurazione. Puoi anche rinominare o eliminare il registratore di configurazione utilizzando AWS CLI l' AWS Config API o uno degli SDK. AWS I seguenti passaggi ti possono essere di aiuto nell'utilizzo di AWS CLI.

To stop the configuration recorder

Utilizza il comando `stop-configuration-recorder`:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

To start the configuration recorder

Utilizza il comando `start-configuration-recorder`:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

To change the recording frequency

Utilizza il comando `put-configuration-recorder` per modificare la frequenza di registrazione per il registratore di configurazione:

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json
```

Il `configurationRecorder.json` file specifica `name` e la frequenza `roleArn` di registrazione predefinita per il registratore di configurazione (). `recordingMode` È inoltre possibile utilizzare questo campo per sovrascrivere la frequenza di registrazione per tipi di risorse specifici.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in
 the override ]
        }
    ]
  }
}
```

`put-configuration-recorder` usa i seguenti campi per il parametro `--configuration-recorder`:

- `name`— Il nome del registratore di configurazione. AWS Config assegna automaticamente il nome di «default» durante la creazione del registratore di configurazione.
- `roleARN`— Amazon Resource Name (ARN) del ruolo IAM assunto AWS Config e utilizzato dal registratore di configurazione.
- `recordingMode`— Speciifica la frequenza di registrazione predefinita AWS Config utilizzata per registrare le modifiche alla configurazione. AWS Config supporta la registrazione continua e la registrazione giornaliera. La registrazione continua consente di registrare continuamente le modifiche alla configurazione ogni volta che si verifica una modifica. La registrazione giornaliera consente di ricevere un elemento di configurazione (CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza.
  - `recordingFrequency`— La frequenza di registrazione predefinita AWS Config utilizzata per registrare le modifiche alla configurazione.

    > **Note**
    >
    > AWS Firewall Manager dipende dalla registrazione continua per monitorare le risorse. Se si utilizza Firewall Manager, si consiglia di impostare la frequenza di registrazione su Continuo.

  - `recordingModeOverrides`: questo campo consente di specificare le sostituzioni per la modalità di registrazione. Si tratta di un array di oggetti `recordingModeOverride`. Ogni oggetto `recordingModeOverride` dell'array `recordingModeOverrides` è composto da tre campi:
    - `description`— Una descrizione fornita per l'override.
    - `recordingFrequency`— La frequenza di registrazione che verrà applicata a tutti i tipi di risorse specificati nell'override.
    - `resourceTypes`— Un elenco separato da virgole che specifica quali tipi di risorse sono AWS Config inclusi nell'override.

> **Note**
>
> Campi obbligatori e facoltativi

Il campo `recordingMode` per `put-configuration-recorder` è facoltativo. Per impostazione predefinita, la frequenza di registrazione per il registratore di configurazione è impostata su Registrazione continua.

> **Note**
>
> Limiti
>
> La registrazione giornaliera non è supportata per i tipi di risorse seguenti:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> Per la strategia di registrazione Registra tutti i tipi di risorse supportati attuali e futuri (`ALL_SUPPORTED_RESOURCE_TYPES`), questi tipi di risorse saranno impostati su Registrazione continua.

To delete the configuration recorder

Utilizza il comando `delete-configuration-recorder`:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

To rename the configuration recorder

Per modificare il nome del registratore della configurazione, devi cancellarlo e creare un nuovo registratore della configurazione con il nome desiderato.

1. Utilizza il comando `describe-configuration-recorders` per cercare il nome del tuo registratore della configurazione corrente:

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
```

```
            "name": "default"
        }
    ]
}
```

2. Utilizza il comando `delete-configuration-recorder` per cancellare il tuo registratore della configurazione corrente:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

3. Utilizza il comando `put-configuration-recorder` per creare un registratore della configurazione con il nome desiderato:

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

4. Utilizza il comando `start-configuration-recorder` per riprendere la registrazione:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Rilevamento delle deviazioni del registratore di configurazione

Il tipo di risorsa `AWS::Config::ConfigurationRecorder` è un elemento di configurazione (CI) del registratore di configurazione che tiene traccia di tutte le modifiche allo stato del registratore di configurazione. Puoi utilizzare questo elemento di configurazione per verificare se lo stato del registratore di configurazione è diverso o se ha subito deviazioni rispetto allo stato precedente. Ad esempio, questo CI rileva se sono presenti aggiornamenti ai tipi di risorse di cui è stata abilitata AWS Config la registrazione, se il registratore di configurazione è stato interrotto o avviato o se è stato eliminato o disinstallato il registratore di configurazione. Un registratore di configurazione deviato indica che le modifiche ai tipi di risorse previsti non vengono rilevate con precisione. Se il registratore di configurazione è stato deviato, ciò può comportare risultati di conformità falsi negativi o falsi positivi.

Il tipo di `AWS::Config::ConfigurationRecorder` risorsa è un tipo di risorsa di sistema AWS Config e la registrazione di questo tipo di risorsa è abilitata per impostazione predefinita in tutte le regioni supportate. La registrazione del tipo di risorsa `AWS::Config::ConfigurationRecorder` è disponibile senza costi aggiuntivi.

Gestione del Canale di Distribuzione

Poiché registra AWS Config continuamente le modifiche che si verificano alle AWS risorse, invia notifiche e stati di configurazione aggiornati attraverso il canale di distribuzione. È possibile gestire il canale di distribuzione per controllare dove AWS Config inviare gli aggiornamenti di configurazione.

È possibile disporre di un solo canale di consegna per AWS Account AWS regione e il canale di consegna deve essere utilizzato AWS Config.

Quando AWS Config rileva una modifica della configurazione per una risorsa e la notifica supera la dimensione massima consentita da Amazon SNS, la notifica include un breve riepilogo dell'elemento di configurazione. Puoi visualizzare la notifica completa seguendo il percorso del bucket Amazon S3 indicato nel campo `s3BucketLocation`. Per ulteriori informazioni, consulta Esempio di notifica della modifica di un elemento della configurazione sovradimensionato.

> **Note**
>
> AWS Config supporta AWS KMS la crittografia per i bucket Amazon S3 utilizzati da AWS Config
> Puoi fornire una chiave AWS Key Management Service (AWS KMS) o un alias Amazon Resource Name (ARN) per crittografare i dati forniti al tuo bucket Amazon Simple Storage Service (Amazon S3). Per impostazione predefinita, AWS Config fornisce la cronologia di configurazione e i file di snapshot al bucket Amazon S3 e crittografa i dati inattivi utilizzando la crittografia lato server S3 AES-256, SSE-S3. Tuttavia, se fornisci AWS Config la tua chiave KMS o l'alias ARN, AWS Config utilizza quella chiave KMS anziché la crittografia AES-256.
> AWS Config non supporta il canale di distribuzione verso un bucket Amazon S3 in cui il blocco degli oggetti è abilitato con la conservazione predefinita abilitata. Per ulteriori informazioni, consulta Come funziona il blocco oggetti S3.

Argomenti

- Terminologia
- Aggiornamento del Canale di Distribuzione
- Ridenominazione del Canale di Distribuzione
- Componenti di un elemento di configurazione
- Distribuzione di istantanee di configurazione a un bucket Amazon S3

- Notifiche che AWS Config Invia a un argomento Amazon SNS

Terminologia

Un elemento di configurazione rappresenta una point-in-time visualizzazione dei vari attributi di una AWS risorsa supportata presente nel tuo account. I componenti di un elemento di configurazione includono metadati, attributi, relazioni, configurazione corrente ed eventi correlati. AWS Config crea un elemento di configurazione ogni volta che rileva una modifica a un tipo di risorsa che sta registrando. Ad esempio, se AWS Config sta registrando bucket Amazon S3, AWS Config crea un elemento di configurazione ogni volta che un bucket viene creato, aggiornato o eliminato. Puoi anche scegliere di creare un elemento AWS Config di configurazione alla frequenza di registrazione che hai impostato.

Una cronologia della configurazione è una raccolta di elementi della configurazione per una data risorsa durante un qualsiasi periodo di tempo. Una cronologia della configurazione può aiutarti a rispondere a domande relative, ad esempio, a quando la risorsa è stata creata per la prima volta, al modo in cui la risorsa è stata configurata durante l'ultimo mese e alle modifiche della configurazione che sono state apportate ieri alle 9 di mattina. La cronologia delle configurazioni è disponibile in diversi formati. AWS Config fornisce automaticamente un file di cronologia della configurazione per ogni tipo di risorsa che viene registrato in un bucket Amazon S3 specificato. Puoi selezionare una determinata risorsa nella AWS Config console e passare a tutti gli elementi di configurazione precedenti per quella risorsa utilizzando la sequenza temporale. Inoltre, puoi accedere allo storico degli elementi della configurazione di una risorsa tramite l'API.

Uno snapshot della configurazione è una raccolta degli elementi della configurazione per tutte le risorse supportate presenti nel tuo account. Questo snapshot della configurazione fornisce un quadro completo delle risorse che vengono registrate e delle loro configurazioni. Lo snapshot della configurazione può essere uno strumento utile per convalidare la configurazione. Ad esempio, puoi esaminare regolarmente lo snapshot della configurazione alla ricerca di risorse che siano state configurate non correttamente o che, potenzialmente, non dovrebbero esistere. Lo snapshot della configurazione è disponibile in più formati. Puoi distribuire lo snapshot della configurazione su un bucket Amazon Simple Storage Service (Amazon S3) di tua scelta. Inoltre, puoi selezionare un momento temporale nella AWS Config console e navigare nell'istantanea degli elementi di configurazione utilizzando le relazioni tra le risorse.

Un flusso di configurazione è un elenco aggiornato automaticamente di tutti gli elementi di configurazione per le risorse in fase AWS Config di registrazione. Ogni volta che una risorsa viene creato, modificata o eliminata, AWS Config crea un elemento della configurazione e lo aggiunge al

flusso di configurazione. Il flusso di configurazione funziona utilizzando un argomento Amazon Simple Notification Service (Amazon SNS) di tua scelta. Il flusso di configurazione è utile per osservare le modifiche alla configurazione man mano che si verificano in modo da individuare potenziali problemi, generare notifiche se determinate risorse vengono modificate o aggiornare sistemi esterni che devono riflettere la configurazione delle AWS risorse.

Aggiornamento del Canale di Distribuzione

Quando aggiorni il canale di distribuzione, puoi specificare le seguenti opzioni:

- Il bucket Amazon S3 a cui AWS Config inviare istantanee di configurazione e file di cronologia delle configurazioni.
- Con quale frequenza AWS Config fornisce istantanee di configurazione al tuo bucket Amazon S3.
- L'argomento Amazon SNS a cui AWS Config inviare notifiche sulle modifiche alla configurazione.

Per aggiornare il canale di distribuzione (console)

Puoi utilizzare la AWS Config console per impostare il bucket Amazon S3 e l'argomento Amazon SNS per il tuo canale di distribuzione. Per la procedura di gestione di tali impostazioni, vedi Configurazione AWS Config con la console.

La console non fornisce opzioni per rinominare il canale di distribuzione, impostare la frequenza degli snapshot di configurazione o eliminare il canale di distribuzione. Per eseguire queste attività, devi utilizzare l' AWS CLI AWS Config API o uno degli SDK. AWS

Per aggiornare il canale di distribuzione (AWS SDK)

I seguenti esempi di codice mostrano come utilizzare`PutDeliveryChannel`.

CLI

AWS CLI

Per creare un canale di distribuzione

Il comando seguente fornisce le impostazioni per il canale di consegna come codice JSON:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

Il `deliveryChannel.json` file specifica gli attributi del canale di consegna:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

L'esempio seguente imposta i seguenti attributi:

`name`- Il nome del canale di consegna. Per impostazione predefinita, AWS Config assegna il nome `default` a un nuovo canale di consegna. Non è possibile aggiornare il nome del canale di consegna con il comando. `put-delivery-channel` Per i passaggi per modificare il nome, vedi Ridenominazione del canale di consegna. `s3BucketName` - Il nome del bucket Amazon S3 a cui AWS Config fornisce istantanee di configurazione e file di cronologia della configurazione. Se si specifica un bucket che appartiene a un altro AWS account, tale bucket deve disporre di politiche che concedano le autorizzazioni di accesso a Config. AWS Per ulteriori informazioni, consulta Autorizzazioni per il bucket Amazon S3.

`snsTopicARN`- L'Amazon Resource Name (ARN) dell'argomento Amazon SNS a cui AWS Config invia notifiche sulle modifiche alla configurazione. Se scegli un argomento da un altro account, l'argomento deve avere politiche che concedano le autorizzazioni di accesso a Config. AWS Per ulteriori informazioni, consulta l'argomento Autorizzazioni per l'argomento Amazon SNS.

`configSnapshotDeliveryProperties`- Contiene l'`deliveryFrequency`attributo, che imposta la frequenza con cui AWS Config fornisce istantanee di configurazione e la frequenza con cui richiama le valutazioni per le regole Config periodiche.

Se il comando ha esito positivo, AWS Config non restituisce alcun output. Per verificare le impostazioni del tuo canale di consegna, esegui il describe-delivery-channels comando.

- Per i dettagli sull'API, consulta PutDeliveryChannel in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio modifica la proprietà DeliveryFrequency di un canale di consegna esistente.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- Per i dettagli sull'API, vedere PutDeliveryChannel in AWS Tools for PowerShell Cmdlet Reference.

(Facoltativo) Puoi utilizzare il comando `describe-delivery-channels` per verificare che le impostazione del canale di distribuzione siano state aggiornate:

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

I seguenti esempi di codice mostrano come utilizzare. `DescribeDeliveryChannels`

CLI

AWS CLI

Per ottenere dettagli sul canale di distribuzione

Il comando seguente restituisce i dettagli sul canale di consegna:

```
aws configservice describe-delivery-channels
```

Output:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- Per i dettagli sull'API, consulta DescribeDeliveryChannels in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio recupera il canale di consegna per la regione e visualizza i dettagli.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Output:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Per i dettagli sull'API, vedere DescribeDeliveryChannels in AWS Tools for PowerShell Cmdlet Reference.

Ridenominazione del Canale di Distribuzione

Per modificare il nome del canale di distribuzione, devi cancellarlo e creare un nuovo canale di distribuzione con il nome desiderato. Prima di eliminare il canale di distribuzione, devi interrompere temporaneamente la registrazione della configurazione.

La AWS Config console non offre la possibilità di eliminare il canale di distribuzione, quindi è necessario utilizzare la AWS CLI, l' AWS Config API o uno degli AWS SDK.

Per rinominare il canale di distribuzione (AWS CLI)

Rinominare il canale di distribuzione utilizzando il AWS CLI

1. Utilizzare il comando `stop-configuration-recorder` per arrestare la registrazione della configurazione:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

2. Utilizzare il comando `describe-delivery-channels` e prendere nota degli attributi del canale di distribuzione:

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

3. Utilizzare il comando `delete-delivery-channel` per eliminare il canale di distribuzione:

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. Utilizzare il comando `put-delivery-channel` per creare un canale di distribuzione con il nome desiderato:

```
$ aws configservice put-delivery-channel --delivery-channel file:// deliveryChannel.json
```

Il file deliveryChannel.json specifica gli attributi del canale di distribuzione:

```
{
    "name": "myCustomDeliveryChannelName",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

5. Utilizza il comando `start-configuration-recorder` per riprendere la registrazione:

```
$ aws configservice start-configuration-recorder --configuration-recorder-name configRecorderName
```

Componenti di un elemento di configurazione

Un elemento di configurazione rappresenta una point-in-time visualizzazione dei vari attributi di una AWS risorsa supportata presente nel tuo account. I componenti di un elemento di configurazione includono metadati, attributi, relazioni, configurazione corrente ed eventi correlati. AWS Config crea un elemento di configurazione ogni volta che rileva una modifica a un tipo di risorsa che sta registrando. Ad esempio, se AWS Config sta registrando bucket Amazon S3, AWS Config crea un elemento di configurazione ogni volta che un bucket viene creato, aggiornato o eliminato. Puoi anche scegliere di creare un elemento AWS Config di configurazione alla frequenza di registrazione che hai impostato.

Un elemento di configurazione è costituito dai componenti seguenti.

Componente	Descrizione	Contiene
Metadati	Informazioni su questo elemento di configurazione	• ID versione • Ora in cui l'elemento di configurazione è stato acquisito • Stato dell'elemento di configurazione che indica se l'elemento è stato acquisito con successo • Stato ID che indica l'ordine degli elementi di configurazione di una risorsa
Attributes	Attributi delle risorse	• ID risorsa • Elenco di tag chiave-valore per questa risorsa • Tipo di risorsa (vediTipi di risorsa supportati) • Nome della risorsa Amazon (ARN) • Zona di disponibilità che contiene la risorsa, se applicabile • Ora in cui è stata creata la risorsa
Relazioni	In che modo la risorsa è correlata ad altre risorse associate all'account	Descrizione della relazione, ad esempio il volume Amazon EBS `vol-1234567` collegato a un'istanza Amazon EC2 `i-a1b2c3d4`
Configurazione attuale	Informazioni restituite tramite una chiamata all'API Describe o List della risorsa	Ad esempio, l'API `DescribeVolumes` restituisce le seguenti informazioni sul volume: • Zona di disponibilità in cui si trova il volume • Ora in cui il volume è stato collegato • L'ID dell'istanza EC2 è collegato a • Stato corrente del volume

Componente	Descrizione	Contiene
		• Stato di DeleteOnTermination bandiera • Dispositivo a cui è collegato il volume • Tipo di volume, ad esempio `gp2`, `io1`, o `standard`

Note

1. Una relazione dell'elemento di configurazione non include il flusso di rete o le dipendenze del flusso di dati. Gli elementi di configurazione non possono essere personalizzati per rappresentare l'architettura della tua applicazione.
2. A partire dalla versione 1.3, il campo relatedEvents è vuoto. Puoi accedere all'LookupEvents API nell'AWS CloudTrail API Reference per recuperare gli eventi per la risorsa.
3. A partire dalla versione 1.3, il campo configurationItemMD5Hash è vuoto. Puoi utilizzare il configurationStateId campo per assicurarti di disporre dell'elemento di configurazione più recente.

Distribuzione di istantanee di configurazione a un bucket Amazon S3

AWS Config fornisce istantanee di configurazione delle AWS risorse registrate AWS Config nel bucket Amazon S3 specificato al momento della configurazione del canale di distribuzione.

Argomenti

- Distribuzione di istantanee di configurazione
- Esempio di istantanea di configurazione da AWS Config
- Verifica dello stato della distribuzione
- Visualizzazione di uno snapshot di configurazione nel bucket Amazon S3

Distribuzione di istantanee di configurazione

AWS Config genera istantanee di configurazione quando si richiama l'azione DeliverConfigSnapshot o si esegue il comando. AWS CLI `deliver-config-snapshot` AWS Config archivia gli snapshot di configurazione nel bucket Amazon S3 che hai specificato al momento dell'attivazione. AWS Config

Digita il `deliver-config-snapshot`comando specificando il nome assegnato da AWS Config quando hai configurato il canale di distribuzione, ad esempio:

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}
```

Esempio di istantanea di configurazione da AWS Config

Di seguito è riportato un esempio delle informazioni AWS Config incluse in uno snapshot di configurazione. L'istantanea descrive la configurazione delle risorse che AWS Config vengono registrate nell'area corrente dell'utente Account AWS e descrive le relazioni tra queste risorse.

> **Note**
>
> Lo snapshot di configurazione può includere riferimenti a tipi di risorse e ID delle risorse che non sono supportati.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
```

```
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "i-344c463d",
            "accountId": "12345678910",
            "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
            "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
            "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
            "configurationItemStatus": "OK",
```

```
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Instance",
            "resourceCreationTime": "2014-02-26T22:56:35.000Z",
            "tags": {
                "Name": "integ-test-1",
                "examplename": "examplevalue"
            },
            "relationships": [
                {
                    "resourceId": "vol-ce676ccc",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume"
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
```

```
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
                    "availabilityZone": "us-west-2b",
                    "groupName": "",
                    "tenancy": "default"
                },
                "kernelId": "aki-fc8f11cc",
                "monitoring": {
                    "state": "disabled"
                },
                "subnetId": "subnet-47b4cf2c",
                "vpcId": "vpc-41b4cf2a",
                "privateIpAddress": "172.31.21.63",
                "publicIpAddress": "54.218.4.189",
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/sda1",
                "blockDeviceMappings": [
                    {
                        "deviceName": "/dev/sda1",
                        "ebs": {
                            "volumeId": "vol-ef0e06ed",
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:38.0000+0000",
                            "deleteOnTermination": true
                        }
                    },
                    {
                        "deviceName": "/dev/sdf",
                        "ebs": {
                            "volumeId": "vol-ce676ccc",
                            "status": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    }
                ],
                "virtualizationType": "paravirtual",
                "clientToken": "aBCDe123456",
                "tags": [
                    {
                        "key": "Name",
                        "value": "integ-test-1"
                    },
```

```
                    {
                        "key": "examplekey",
                        "value": "examplevalue"
                    }
                ],
                "securityGroups": [
                    {
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
```

```
                            {
                                "privateIpAddress": "172.31.21.63",
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```

Il passaggio successivo è quello di verificare che lo snapshot di configurazione sia correttamente consegnato al canale di distribuzione.

Verifica dello stato della distribuzione

Digita il `describe-delivery-channel-status`comando per verificare che AWS Config abbia iniziato a fornire le configurazioni al canale di consegna specificato, ad esempio:

```
$ aws configservice describe-delivery-channel-status
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
                "lastStatus": "SUCCESS"
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
            },
            "configSnapshotDeliveryInfo": {
```

```
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415333113.4159999
            },
            "name": "default"
        }
    ]
}
```

La risposta elenca lo stato di tutti e tre i formati di consegna AWS Config utilizzati per fornire le configurazioni al tuo bucket e all'argomento.

Dai un'occhiata al campo `lastSuccessfulTime` in `configSnapshotDeliveryInfo`. L'ora deve corrispondere al momento dell'ultima richiesta di distribuzione dello snapshot di configurazione.

> **Note**
>
> AWS Config utilizza il formato UTC (Coordinated Universal Time) per registrare l'ora.

Visualizzazione di uno snapshot di configurazione nel bucket Amazon S3

1. Accedi AWS Management Console e apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
2. Nell'elenco Tutti i bucket della console Amazon S3, fai clic sul nome del bucket Amazon S3.
3. Fare clic attraverso le cartelle nidificate nel bucket fino a visualizzare l'oggetto `ConfigSnapshot` con un ID snapshot corrispondente all'ID restituito dal comando. Scaricare e aprire l'oggetto per visualizzare lo snapshot di configurazione.

   Il bucket S3 contiene anche un file vuoto denominato. `ConfigWritabilityCheckFile` AWS Config crea questo file per verificare che il servizio sia in grado di scrivere correttamente nel bucket S3.

Notifiche che AWS Config Invia a un argomento Amazon SNS

> **Note**
>
> Prima di AWS Config poter inviare notifiche a un argomento di Amazon SNS, devi prima configurare il registratore di configurazione e il canale di distribuzione. Per ulteriori informazioni, consulta Gestione del registratore di configurazione e Gestione del canale di distribuzione.

È possibile configurare AWS Config affinché invii le modifiche della configurazione e le notifiche a un argomento Amazon SNS. Ad esempio, quando una risorsa viene aggiornata, puoi ricevere una notifica al tuo indirizzo email, in modo che tu possa visualizzare tali modifiche. Puoi inoltre ricevere una notifica quando AWS Config valuta le risorse rispetto alle regole personalizzate o gestite. Per ulteriori informazioni, vedere Logging and Monitoring in. AWS Config

AWS Config invia notifiche per gli eventi seguenti:

- Modifica di un elemento della configurazione per una risorsa.
- Distribuzione all'account della cronologia della configurazione di una risorsa.
- Avvio e distribuzione all'account dello snapshot di configurazione di una risorsa registrata.
- Stato di conformità delle risorse e loro conformità rispetto alle tue regole.
- Inizio della valutazione di una risorsa rispetto a una regola.
- AWS Config non è riuscito a distribuire la notifica al tuo account.

Argomenti

- Esempio notifiche di modifica di un elemento della configurazione
- Esempio di notifica della distribuzione della cronologia della configurazione
- Esempio di notifica dell'avvio della distribuzione dello snapshot della configurazione
- Esempio di notifica della distribuzione dello snapshot della configurazione
- Esempio di notifica della modifica della conformità
- Esempio di notifica dell'avvio della valutazione delle regole
- Esempio di notifica della modifica di un elemento della configurazione sovradimensionato
- Esempio di notifica della distribuzione non conclusa correttamente

Esempio notifiche di modifica di un elemento della configurazione

AWS Config utilizza Amazon SNS per inviare notifiche agli endpoint dell'abbonamento. Queste notifiche forniscono lo stato di consegna degli snapshot e delle cronologie di configurazione e forniscono ogni elemento di configurazione che si AWS Config crea quando le configurazioni delle risorse registrate cambiano. AWS AWS Config invia anche notifiche che mostrano se le risorse sono conformi alle regole. Se decidi di inviare notifiche via email, nella tua applicazione client di posta elettronica puoi applicare i filtri al contenuto dell'oggetto e del testo del messaggio email.

Di seguito è riportato un esempio di payload di una notifica Amazon SNS generata quando AWS Config rileva che il volume Amazon Elastic Block Store `vol-ce676ccc` viene associato all'istanza con ID `i-344c463d`. La notifica contiene la modifica dell'elemento della configurazione per la risorsa.

```
{
    "Type": "Notification",
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "accountId": "123456789012",
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
                        "resourceId": "i-344c463d",
                        "resourceType": "AWS::EC2::INSTANCE",
                        "name": "Attached to Instance"
                    }
```

```
                ],
                "configuration": {
                    "volumeId": "vol-ce676ccc",
                    "size": 1,
                    "snapshotId": "",
                    "availabilityZone": "us-west-2b",
                    "state": "in-use",
                    "createTime": "2014-02-27T21:43:53.0885+0000",
                    "attachments": [
                        {
                            "volumeId": "vol-ce676ccc",
                            "instanceId": "i-344c463d",
                            "device": "/dev/sdf",
                            "state": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    ],
                    "tags": [],
                    "volumeType": "standard"
                }
            }
        ],
        "configurationItemDiff": {
            "changeType": "UPDATE",
            "changedProperties": {
                "Configuration.State": {
                    "previousValue": "available",
                    "updatedValue": "in-use",
                    "changeType": "UPDATE"
                },
                "Configuration.Attachments.0": {
                    "updatedValue": {
                        "VolumeId": "vol-ce676ccc",
                        "InstanceId": "i-344c463d",
                        "Device": "/dev/sdf",
                        "State": "attached",
                        "AttachTime": "FriMar0723: 46: 28UTC2014",
                        "DeleteOnTermination": "false"
                    },
                    "changeType": "CREATE"
                }
            }
        }
```

```
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```

Elementi di configurazione per risorse legate da relazioni

Se una risorsa è in relazione con altre risorse, una modifica a tale risorsa può determinare la creazione di molteplici elementi di configurazione. L'esempio seguente mostra come AWS Config crea elementi di configurazione per risorse con relazioni.

1. Hai un'istanza Amazon EC2 con ID `i-007d374c8912e3e90` e l'istanza è associata a un gruppo di sicurezza Amazon EC2, `sg-c8b141b4`.
2. Puoi aggiornare la tua istanza EC2 per modificare il gruppo di sicurezza impostando un altro gruppo di sicurezza, `sg-3f1fef43`.
3. Poiché l'istanza EC2 è correlata a un'altra risorsa, AWS Config crea più elementi di configurazione come negli esempi seguenti:

Questa notifica contiene la modifica dell'elemento della configurazione dell'istanza EC2 derivata dalla sostituzione del gruppo di sicurezza.

```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
 in Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {
```

```
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-1",
                            "groupId": "sg-c8b141b4"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
```

```
                "Relationships.0": {
                    "previousValue": {
                        "resourceId": "sg-c8b141b4",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Configuration.NetworkInterfaces.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-2",
                            "groupId": "sg-3f1fef43"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
```

```
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "changeType": "CREATE"
                },
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.0": {
                    "previousValue": {
                        "groupName": "example-security-group-1",
                        "groupId": "sg-c8b141b4"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                }
            },
            "changeType": "UPDATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [
                {
                    "resourceId": "eni-fde9493f",
```

```
                "resourceName": null,
                "resourceType": "AWS::EC2::NetworkInterface",
                "name": "Contains NetworkInterface"
            },
            {
                "resourceId": "sg-3f1fef43",
                "resourceName": null,
                "resourceType": "AWS::EC2::SecurityGroup",
                "name": "Is associated with SecurityGroup"
            },
            {
                "resourceId": "subnet-2372be7b",
                "resourceName": null,
                "resourceType": "AWS::EC2::Subnet",
                "name": "Is contained in Subnet"
            },
            {
                "resourceId": "vol-0a2d63a256bce35c5",
                "resourceName": null,
                "resourceType": "AWS::EC2::Volume",
                "name": "Is attached to Volume"
            },
            {
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }
        ],
        "configuration": {
            "instanceId": "i-007d374c8912e3e90",
            "imageId": "ami-9be6f38c",
            "state": {
                "code": 16,
                "name": "running"
            },
            "privateDnsName": "ip-172-31-16-84.ec2.internal",
            "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
            "stateTransitionReason": "",
            "keyName": "ec2-micro",
            "amiLaunchIndex": 0,
            "productCodes": [],
            "instanceType": "t2.micro",
            "launchTime": "2017-01-09T20:13:28.000Z",
```

```
                "placement": {
                    "availabilityZone": "us-east-2c",
                    "groupName": "",
                    "tenancy": "default",
                    "hostId": null,
                    "affinity": null
                },
                "kernelId": null,
                "ramdiskId": null,
                "platform": null,
                "monitoring": {"state": "disabled"},
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "privateIpAddress": "172.31.16.84",
                "publicIpAddress": "54.175.43.43",
                "stateReason": null,
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/xvda",
                "blockDeviceMappings": [{
                    "deviceName": "/dev/xvda",
                    "ebs": {
                        "volumeId": "vol-0a2d63a256bce35c5",
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:03.000Z",
                        "deleteOnTermination": true
                    }
                }],
                "virtualizationType": "hvm",
                "instanceLifecycle": null,
                "spotInstanceRequestId": null,
                "clientToken": "bIYqA1483990561516",
                "tags": [{
                    "key": "Name",
                    "value": "value"
                }],
                "securityGroups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [{
                    "networkInterfaceId": "eni-fde9493f",
```

```
                    "subnetId": "subnet-2372be7b",
                    "vpcId": "vpc-14400670",
                    "description": "",
                    "ownerId": "123456789012",
                    "status": "in-use",
                    "macAddress": "0e:36:a2:2d:c5:e0",
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
                    "sourceDestCheck": true,
                    "groups": [{
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    }],
                    "attachment": {
                        "attachmentId": "eni-attach-85bd89d9",
                        "deviceIndex": 0,
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:02.000Z",
                        "deleteOnTermination": true
                    },
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    },
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
                "sriovNetSupport": null,
                "enaSupport": true
            },
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
```

```
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Questa notifica contiene la modifica dell'elemento della configurazione del gruppo di sicurezza dell'istanza EC2, `sg-3f1fef43`, che è associato all'istanza.


```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
```

```
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }],
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
                "vpcId": "vpc-14400670",
                "tags": []
            },
            "supplementaryConfiguration": {},
            "tags": {},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
```

```
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Comprensione del campo **`configurationItemDiff`** nelle notifiche **`ConfigurationItemChangeNotification`** di Amazon SNS

AWS Config crea un elemento di configurazione ogni volta che la configurazione di una risorsa cambia (create/update/delete). Per un elenco dei tipi di risorse supportati che possono registrare, vedere. AWS Config Tipi di risorsa supportati AWS Config utilizza Amazon SNS per inviare una notifica man mano che vengono apportate le modifiche. Il payload di notifica di Amazon SNS include campi per aiutarti a tenere traccia delle modifiche alle risorse in una determinata regione. AWS

Per capire perché ricevi una notifica `ConfigurationItemChangeNotification`, rivedi i dettagli `configurationItemDiff`. I campi variano a seconda del tipo di modifica e possono formare diverse combinazioni come UPDATE-UPDATE, UPDATE-CREATE e DELETE-DELETE. Di seguito sono riportate le spiegazioni di alcune combinazioni comuni.

UPDATE-CREATE e UPDATE-UPDATE

L'esempio seguente include le modifiche alle relazioni dirette delle risorse e alle configurazioni delle risorse. I dettagli `configurationItemDiff` rivelano le seguenti informazioni:

Azione eseguita: una policy gestita presente nell'account è stata allegata a un ruolo AWS Identity and Access Management (IAM).

Operazione di base eseguita: UPDATE (aggiornamento del numero di associazioni del tipo di risorsa `AWS::IAM::Policy` in un account).

Combinazioni di tipi di modifica:

1. Modifica delle relazioni dirette delle risorse UPDATE-CREATE. È stato creato un nuovo collegamento o associazione tra una policy IAM e un ruolo IAM.
2. Modifica della configurazione delle risorse UPDATE-UPDATE. Il numero di associazioni di policy IAM è passato da 2 a 3 quando la policy è stata associata al ruolo IAM.

Esempio di notifica `configurationItemDiff` UPDATE-CREATE e UPDATE-UPDATE:

```
{
    "configurationItemDiff": {
        "changedProperties": {
            "Relationships.0": {
                "previousValue": null,
                "updatedValue": {
                    "resourceId": "AROA6D3M4S53*********",
                    "resourceName": "Test1",
                    "resourceType": "AWS::IAM::Role",
                    "name": "Is attached to Role"
                },
                "changeType": "CREATE"                >>>>>>>>>>>>>>>>>>>> 1
            },
            "Configuration.AttachmentCount": {
                "previousValue": 2,
                "updatedValue": 3,
                "changeType": "UPDATE"                >>>>>>>>>>>>>>>>>>>> 2
            }
        },
        "changeType": "UPDATE"
    }
}
```

UPDATE-DELETE

L'esempio seguente include le modifiche alle relazioni dirette delle risorse e alle configurazioni delle risorse. I dettagli `configurationItemDiff` rivelano le seguenti informazioni:

Operazione eseguita: una policy gestita presente nell'account è stata scollegata da un utente IAM.

Operazione di base eseguita: UPDATE (aggiornamento della policy di autorizzazioni associata al tipo di risorsa `AWS::IAM::User`).

Combinazioni di tipi di modifica: modifica delle relazioni dirette delle risorse UPDATE-DELETE. L'associazione tra un utente IAM e una policy IAM in un account è stata eliminata.

Esempio di notifica `configurationItemDiff` UPDATE-DELETE:

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Configuration.UserPolicyList.0": {
        "previousValue": {
          "policyName": "Test2",
          "policyDocument": "{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/VPCId": "*"
                }
            }
        }
    ]
}"
        },
        "updatedValue": null,
        "changeType": "DELETE"                        >>>>>>>>>>>>>>>>>>>> 3
      }
    },
    "changeType": "UPDATE"
  }
}
```

DELETE-DELETE

L'esempio seguente include le modifiche alle relazioni dirette delle risorse e alle configurazioni delle risorse. I dettagli `configurationItemDiff` rivelano le seguenti informazioni:

Operazione eseguita: un ruolo IAM presente in un account è stato eliminato.

Operazione di base eseguita: DELETE (una risorsa del tipo di risorsa `AWS::IAM::Role` è stata eliminata).

Combinazioni di tipi di modifica: modifica delle relazioni dirette delle risorse e modifica della configurazione delle risorse DELETE-DELETE. L'eliminazione del ruolo IAM ha eliminato anche l'associazione della policy IAM al ruolo IAM.

Esempio di notifica `configurationItemDiff` DELETE-DELETE:

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Relationships.0": {
        "previousValue": {
          "resourceId": "ANPAIJ5MXUKK*********",
          "resourceName": "AWSCloudTrailAccessPolicy",
          "resourceType": "AWS::IAM::Policy",
          "name": "Is attached to CustomerManagedPolicy"
        },
        "updatedValue": null,
        "changeType": "DELETE"
      },
      "Configuration": {
        "previousValue": {
          "path": "/",
          "roleName": "CloudTrailRole",
          "roleId": "AROAJITJ6YGM*********",
          "arn": "arn:aws:iam::123456789012:role/CloudTrailRole",
          "createDate": "2017-12-06T10:27:51.000Z",
          "assumeRolePolicyDocument": "{"Version":"2012-10-17","Statement":
[{"Sid":"","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"sts:AssumeRole","Condition":
{"StringEquals":{"sts:ExternalId":"123456"}}}]}",
          "instanceProfileList": [],
          "rolePolicyList": [],
          "attachedManagedPolicies": [
            {
              "policyName": "AWSCloudTrailAccessPolicy",
              "policyArn": "arn:aws:iam::123456789012:policy/AWSCloudTrailAccessPolicy"
            }
          ],
          "permissionsBoundary": null,
          "tags": [],
```

```
          "roleLastUsed": null
        },
        "updatedValue": null,
        "changeType": "DELETE"
      }
    },
    "changeType": "DELETE"
}
```

Esempio di notifica della distribuzione della cronologia della configurazione

La cronologia della configurazione è una raccolta di elementi della configurazione per un tipo di risorsa durante un intervallo di tempo. Di seguito è riportato un esempio di notifica che viene AWS Config inviata quando la cronologia di configurazione di una risorsa CloudTrail trail viene consegnata all'account.

```
{
    "Type": "Notification",
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for
 Account 123456789012",
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhr
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Esempio di notifica dell'avvio della distribuzione dello snapshot della configurazione

Questo è un esempio di notifica che AWS Config invia quando AWS Config avvia la distribuzione dello snapshot della configurazione al tuo account.


```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Esempio di notifica della distribuzione dello snapshot della configurazione

Lo snapshot della configurazione è una raccolta di elementi della configurazione per tutte le risorse registrate e le relative configurazioni nel tuo account. Questo è un esempio di notifica che AWS Config invia quando la distribuzione dello snapshot della configurazione al tuo account è completata.


```
{
    "Type": "Notification",
```

```
    "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T18:39:39.853Z",
        "messageType": "ConfigurationSnapshotDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T18:39:40.062Z",
    "SignatureVersion": "1",
    "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKZi+RJQRnDJkL2qb
+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y+tRvmMLY5CI1cYrnuPRhTLdUk+R0sshg5G+JMtSLVG/
TvWbjz44CKXJprjIQg==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Esempio di notifica della modifica della conformità

Quando AWS Config valuta le tue risorse rispetto a una regola personalizzata o gestita, AWS Config invia una notifica che indica se le risorse sono conformi rispetto alla regola.

Di seguito è riportato un esempio di notifica in cui la risorsa CloudTrail trail è conforme alla regola `cloudtrail-enabled` gestita.


```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
```

```
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
```

```
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Esempio: modifica dell'elemento di configurazione Config | Amazon EventBridge


```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
  "detail-type": "Config Configuration Item Change",
  "source": "aws.config",
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
        }
      },
      "changeType": "UPDATE"
    },
```

```
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
        "LifecyclePolicies": [{
          "TransitionToIA": "AFTER_30_DAYS"
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
```

```
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
    }
  }
}
```

Esempio di notifica dell'avvio della valutazione delle regole

AWS Config invia una notifica all'avvio della valutazione delle risorse rispetto a una regola personalizzata o gestita. Qui di seguito è riportato un esempio di notifica inviata quando AWS Config inizia a valutare la regola gestita `iam-password-policy`.

```
{
    "Type": "Notification",
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM
+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
```

```
}
```

Esempio di notifica della modifica di un elemento della configurazione sovradimensionato

Quando AWS Config rileva una modifica della configurazione per una risorsa, invia una notifica relativa all'elemento della configurazione. Se la notifica supera la dimensione massima consentita da Amazon Simple Notification Service (Amazon SNS), la notifica include un breve riepilogo dell'elemento di configurazione. Puoi visualizzare la notifica completa nella posizione del bucket Amazon S3 specificata nel campo. `s3BucketLocation`

Il seguente esempio di notifica mostra un elemento di configurazione per un'istanza Amazon EC2. La notifica include un riepilogo delle modifiche e la posizione della notifica nel bucket Amazon S3.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z

    The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
```

```
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": "my-bucket/AWSLogs/123456789012/Config/
us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

Esempio di notifica della distribuzione non conclusa correttamente

AWS Configinvia una notifica di consegna non riuscita se non è AWS Config possibile inviare lo snapshot di configurazione o una notifica di modifica di un elemento di configurazione sovradimensionato al bucket Amazon S3. Verifica di aver specificato un bucket Amazon S3 valido.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

     The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
```

```
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
      "notificationCreationTime": "2016-10-06T16:46:13.749Z",
      "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
      "recordVersion": "1.0"
    }
```

Gestione e visualizzazione AWS delle configurazioni delle risorse con AWS Config

AWS Config consente di valutare, controllare e valutare le configurazioni delle AWS risorse.

AWS le risorse sono entità che crei e gestisci utilizzando AWS Command Line Interface (CLI), gli AWS SDK o AWS gli strumenti dei partner. AWS Management Console Esempi di AWS risorse includono istanze Amazon EC2, gruppi di sicurezza, Amazon VPC e Amazon Elastic Block Store. AWS Config si riferisce a ciascuna risorsa utilizzando il suo identificatore univoco, come l'ID della risorsa o un Amazon Resource Name (ARN).

Alcuni casi d'uso comuni includono:

- Amministratore cloud: puoi monitorare e gestire le configurazioni delle risorse per garantire la conformità, risolvere i problemi e mantenere una comprensione del tuo ambiente AWS
- Analista della sicurezza: puoi valutare le configurazioni delle risorse rispetto agli stati desiderati per identificare le vulnerabilità e valutare il livello di sicurezza.
- Responsabile della conformità: è possibile controllare e monitorare continuamente le configurazioni delle risorse per garantire il rispetto delle politiche organizzative e degli standard di settore.

Argomenti

- Visualizzazione del AWS Config pannello di controllo
- Tipi di risorsa supportati
- Copertura delle risorse in base alla disponibilità nelle regioni
- AWS Risorse per la registrazione
- Registrazione delle configurazioni per le risorse di terze parti
- Registrazione della configurazione del software per le istanze gestite
- Visualizzazione delle configurazioni e della cronologia delle risorse di
- Tagging delle risorse AWS Config

Visualizzazione del AWS Config pannello di controllo

Usa la dashboard per visualizzare una panoramica delle tue risorse, regole, pacchetti di conformità e relativi stati di conformità e per visualizzare le tue metriche di AWS Config utilizzo e successo con

Amazon. CloudWatch Questa pagina ti aiuta a identificare rapidamente le principali risorse del tuo AWS account, i pacchetti di conformità con il livello di conformità più basso del tuo Account AWS, quali regole o risorse non sono conformi nel tuo account Account AWS, quale traffico determina il tuo AWS Config utilizzo e le metriche chiave di successo e fallimento che si sono verificate nei tuoi flussi di lavoro.

Per utilizzare la Dashboard AWS Config

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Nel riquadro di navigazione a sinistra, seleziona Pannello di controllo.

Indice

- Conformità e inventario risorse
- AWS Config Metriche di utilizzo e successo

Conformità e inventario risorse

Dopo la configurazione, AWS Config inizia a registrare le risorse specificate e a valutarle in base alle regole. Potrebbero essere necessari alcuni minuti AWS Config per visualizzare le risorse, le regole, i pacchetti di conformità e i relativi stati di conformità.

Pacchetti di conformità per punteggio di conformità

In Pacchetti di conformità per punteggio di conformità sono mostrati fino a 10 pacchetti di conformità con il punteggio di conformità più basso. Il punteggio di conformità è la percentuale del numero di combinazioni regola-risorsa conformi in un pacchetto di conformità rispetto al numero totale di combinazioni regola-risorsa possibili nel pacchetto di conformità.

Questa metrica fornisce una visualizzazione di alto livello dello stato di conformità dei pacchetti di conformità e può essere utilizzata per identificare, analizzare e comprendere il livello di conformità dei pacchetti di conformità. Puoi utilizzare il punteggio di conformità per tenere traccia dell'avanzamento delle correzioni, eseguire confronti tra diversi set di requisiti e vedere l'impatto di una modifica o un'implementazione specifica su un pacchetto di conformità.

Per visualizzare lo stato di implementazione, il punteggio di conformità, la relativa timeline e le regole di un pacchetto di conformità in una vista dettagliata, scegli il nome di un pacchetto di conformità in Pacchetto di conformità.

Compliance status (Stato di conformità)

In Stato di conformità è mostrato il numero di regole e risorse conformi e non conformi. Le risorse sono conformi o non conformi in base a una valutazione della regola ad esse associata. Se una risorsa non segue le specifiche della regola, la risorsa e la regola vengono contrassegnate come non conformi.

Per visualizzare l'elenco delle regole e delle risorse non conformi, scegli Regole non conformi o Risorse non conformi.

Regole per risorse non conformi

In Regole per risorse non conformi vengono visualizzate le principali regole non conformi, in ordine decrescente, in base al numero di risorse. Scegli una regola per visualizzarne i dettagli e i parametri e le risorse comprese nel suo ambito.

Per un elenco completo delle regole non conformi, scegli Visualizza tutte le regole non conformi.

Inventario risorse

L'inventario delle risorse mostra il numero totale di risorse registrate AWS Config in ordine decrescente in base al numero di risorse e il conteggio di ogni tipo di risorsa presente nell'inventario. Account AWS Per aprire tutte le risorse per un tipo di risorsa, scegli questo tipo di risorsa per accedere alla relativa pagina Inventario risorse.

Puoi utilizzare l'elenco a discesa per indicare il numero totale delle risorse che desideri visualizzare. Per impostazione predefinita, è impostato per visualizzare tutte le risorse, ma è possibile modificarlo in AWS risorse, Risorse di terze parti o Risorse personalizzate.

> **Note**
>
> Il messaggio Valuta la configurazione AWS delle risorse utilizzando le regole di Config può apparire nella Dashboard per i seguenti motivi:
>
> - Non hai impostato AWS Config le regole per il tuo Account AWS. Puoi selezionare Add rule (Aggiungi regola) per andare alla pagina Rules (Regole).
> - AWS Config sta ancora valutando le tue risorse rispetto alle tue regole. Puoi aggiornare la pagina per vedere gli ultimi risultati della valutazione.
> - AWS Config ha valutato le tue risorse rispetto alle tue regole e non ha trovato alcuna risorsa che rientri nell'ambito. È possibile specificare le risorse AWS Config da registrare

nella pagina Impostazioni. Per ulteriori informazioni, consulta AWS Risorse per la registrazione.

AWS Config Metriche di utilizzo e successo

Puoi utilizzare i CloudWatch dashboard di Amazon nella AWS Config console per visualizzare le tue metriche di AWS Config utilizzo e successo.

Da ciascun pannello di controllo, puoi effettuare le operazioni seguenti:

- Modifica l'intervallo di tempo della dashboard per visualizzare i dati delle ultime 3 ore, 1 giorno o 1 settimana.
- Scegli l'icona del calendario per inserire un intervallo di tempo personalizzato: un tempo relativo per un periodo di tempo specificato in precedenza o un intervallo di tempo assoluto tra due date.
- Puoi modificare il formato dell'ora per visualizzare i dati della dashboard in UTC (Coordinated Universal Time) o nel fuso orario locale (il fuso orario specificato come fuso orario locale nel sistema operativo del dispositivo).
- Utilizzare la freccia a discesa accanto all'icona Aggiorna per specificare la frequenza di aggiornamento dei dati nel pannello di controllo o per disattivare l'aggiornamento automatico. Scegli Disattivato, 10 secondi, 1 minuto, 2 minuti, 5 minuti o 15 minuti per modificare l'intervallo di aggiornamento.
- Scegli Altre opzioni (il menu con i puntini di sospensione verticali) per aggiungere alla console le metriche di AWS Config utilizzo o le metriche di AWS Config successo che stai attualmente visualizzando nella AWS Config Dashboard. CloudWatch Si apre una nuova scheda nella CloudWatch console che ti consente di creare una nuova dashboard personalizzata CloudWatch con le informazioni copiate dalle metriche di AWS Config utilizzo correnti o dalle metriche di successo. AWS Config

Se desideri eseguire analisi aggiuntive di queste metriche con CloudWatch, scegli Metriche nel riquadro di navigazione a sinistra della CloudWatch console, quindi scegli /Config.AWS Per ulteriori informazioni su cosa puoi fare dalla CloudWatch console, consulta Using Amazon CloudWatch dashboards e Using Amazon CloudWatch metrics nella Guida per l'CloudWatch utente.

AWS Config Metriche di utilizzo

Parametro	Descrizione	Unità	
`Configuration Items Recorded`	Il numero di elementi di configurazione registrati per ogni tipo di risorsa o per tutti i tipi di risorse. Un elemento di configurazione rappresenta una point-in-time visualizzazione dei vari attributi di una AWS risorsa supportata. Per ulteriori informazioni sugli elementi di configurazione o sui tipi di risorse supportati, consulta Elementi della configurazione e Tipi di risorsa supportati.	Conteggio	

Puoi selezionare il tipo di risorsa che desideri visualizzare utilizzando l'elenco a discesa. L'impostazione di visualizzazione predefinita è impostata su tutti i tipi di risorse.

AWS Config Metriche di successo

Parametro	Descrizione	Unità	
`Change Notifications Delivery Failed`	Il numero di consegne di notifiche di modifica non riuscite all'argomento Amazon SNS per il tuo canale di consegna. Una notifica di modifica ti informa di una modifica dello stato di configurazione delle tue risorse. AWS Puoi utilizzare l'ConfigStreamDeliveryInfoAPI per ricevere `lastErrorCode` o `lastErrorMessage` inviare l'ultimo tentativo di consegna di una notifica di modifica. Per ulteriori informazioni, consulta Gestione del canale di distribuzione.	Conteggio	
`Config History Export Failed`	Il numero di esportazioni della cronologia di configurazione non riuscite nel tuo bucket Amazon S3. Una cronologia di configurazione è una raccolta di elementi di configurazione	Conteggio	

Parametro	Descrizione	Unità
	per una data risorsa durante un periodo di tempo specificato. Per ulteriori informazioni sulla cronologia di configurazione, consulta Storico della configurazione.	
`Configuration Recorder Insufficient Permissions Failure`	Il numero di tentativi di accesso alle autorizzazioni non riusciti a causa della politica del ruolo IAM per il registratore di configurazione con autorizzazioni insufficienti. Il registratore di configurazione rileva le modifiche alle configurazioni delle risorse e le acquisisce come elementi di configurazione. Affinché il registratore di configurazione registri le configurazioni AWS delle risorse, richiede le autorizzazioni IAM necessarie. Per ulteriori informazioni, consulta Policy del ruolo IAM per il recupero dei dettagli di configurazione.	Conteggio
`Config Snapshot Export Failed`	Il numero di esportazioni di snapshot di configurazione non riuscite nel tuo bucket Amazon S3. Uno snapshot di configurazione è una raccolta degli elementi di configurazione di tutte le risorse supportate nell'account. Per ulteriori informazioni sugli snapshot di configurazione, consulta Snapshot della configurazione.	Conteggio

Tipi di risorsa supportati

> **Important**
>
> Questa pagina viene aggiornata con cadenza mensile all'inizio di ogni mese.

AWS Config supporta i seguenti tipi di AWS risorse e relazioni tra le risorse.

- Per informazioni più dettagliate su un tipo di risorsa, consulta le relative informazioni di riferimento (come sintassi, proprietà e valori restituiti) nel riferimento ai tipi di AWS risorse e proprietà nella Guida per l' AWS CloudFormation utente.
- Per AWS Config la registrazione, alcune AWS regioni supportano un sottoinsieme di questi tipi di risorse. Per informazioni sui tipi di risorse supportati nelle varie regioni, consulta Copertura delle risorse in base alla disponibilità nelle regioni.
- Le interrogazioni avanzate per AWS Config supportano un sottoinsieme di questi tipi di risorse. Per un elenco di tipi di risorsa supportati, consulta Tipi di risorsa supportati per query avanzate.
- La valutazione proattiva per AWS Config supporta un sottoinsieme di questi tipi di risorse. Per un elenco di tipi di risorse supportati, consulta Tipi di risorse supportati per la valutazione proattiva.
- Le regole periodiche vengono eseguite senza che il registratore di configurazione sia abilitato poiché le regole periodiche non dipendono dagli elementi di configurazione. Per ulteriori informazioni sulla differenza tra le regole attivate dal cambiamento e le regole periodiche, vedere Evaluation Mode e Trigger Types for Rules. AWS Config

> **Note**
>
> Prima di specificare un tipo di risorsa da AWS Config monitorare, verifica la disponibilità della copertura delle risorse per regione per verificare se il tipo di risorsa è supportato nella regione in cui è stato configurato AWS . AWS Config Se un tipo di risorsa è supportato da AWS Config almeno una regione, puoi abilitare la registrazione di quel tipo di risorsa in tutte le regioni supportate da AWS Config, anche se il tipo di risorsa specificato non è supportato nella AWS regione in cui è stato AWS Config installato.

Amazon AppStream

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon AppStream	`AWS::AppStream::DirectoryConfig`	N/A	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::AppStream::Application`	ND	ND
	`AWS::AppStream::Stack`	ND	ND
	`AWS::AppStream::Fleet`	ND	N/A

Amazon AppFlow

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon AppFlow	`AWS::AppFlow::Flow`	N/A	N/A

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon AppIntegrations	`AWS::AppIntegrations::EventIntegration`	N/A	N/A

Amazon API Gateway

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
API Gateway	`AWS::ApiGateway::Stage`	è contenuto in	ApiGateway Rest Api
		è associata a	WAFRegional WebACL

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::ApiGateway::RestApi`	contiene	ApiGateway Palco
API Gateway V2	`AWS::ApiGatewayV2::Stage`	è contenuto in	ApiGatewayV2 Api
	`AWS::ApiGatewayV2::Api`	contiene	ApiGatewayFase V2

Per ulteriori informazioni su come AWS Config si integra con Amazon API Gateway, consulta Monitoraggio della configurazione dell'API API Gateway con AWS Config.

Amazon Athena

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Athena	`AWS::Athena::WorkGroup`	N/A	ND
	`AWS::Athena::DataCatalog`	ND	ND
	`AWS::Athena::PreparedStatement`	ND	N/A

Amazon CloudFront

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon CloudFront	`AWS::CloudFront::Distribution`	è associata a	AWS WebACL WAF
			Certificato ACM
			Bucket S3
			Certificato del server di IAM
	`AWS::CloudFront::StreamingDistribution`	è associata a	AWS WebACL WAF
			Certificato ACM
			Bucket S3
			Certificato del server di IAM

Amazon CloudWatch

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	N/A	ND
	`AWS::CloudWatch::MetricStream`	ND	N/A
CloudWatch Registri Amazon	`AWS::Logs::Destination`	N/A	N/A
Amazon CloudWatch RUM	`AWS::RUM::AppMonitor`	N/A	N/A

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon CloudWatch evidentemente	`AWS::Evidently::Project`	N/A	ND
	`AWS::Evidently::Launch`	ND	ND
	`AWS::Evidently::Segment`	ND	N/A

Amazon CodeGuru

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
CodeGuru Revisore Amazon	`AWS::CodeGuruReviewer::RepositoryAssociation`	N/A	N/A
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	N/A	N/A

Amazon Cognito

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Cognito	`AWS::Cognito::UserPool`	N/A	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::Cognito::UserPoolClient`	ND	ND
	`AWS::Cognito::UserPoolGroup`	ND	N/A

Amazon Connect

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Connect	`AWS::Connect::PhoneNumber`	N/A	ND
	`AWS::Connect::QuickConnect`	ND	ND
	`AWS::Connect::Instance`	ND	N/A
Customer Profiles Amazon Connect	`AWS::CustomerProfiles::Domain`	N/A	ND
	`AWS::CustomerProfiles::ObjectType`	ND	N/A

Amazon Detective

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Detective	`AWS::Detective::Graph`	N/A	N/A

Amazon DynamoDB

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon DynamoDB	`AWS::DynamoDB::Table`	N/A	N/A

Amazon Elastic Compute Cloud

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Elastic Compute Cloud	`AWS::EC2::Host` *	contiene	Istanza EC2
	`AWS::EC2::EIP`	è collegata a	Istanza EC2
			Interfaccia di rete
	`AWS::EC2::Instance`	contiene	Interfaccia di rete EC2
		è associata a	Gruppo di sicurezza EC2
		è collegata a	Volume Amazon EBS
			EC2 Elastic IP (EIP)
		è contenuto in	Host dedicato EC2
			Tabella di routing

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
			Sottorete
			Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::EC2::NetworkInterface`	è associata a	Gruppo di sicurezza EC2
		è collegata a	EC2 Elastic IP (EIP)
			Istanza EC2
		è contenuto in	Tabella di routing
			Sottorete
			Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::EC2::SecurityGroup` *	è associata a	Istanza EC2
			Interfaccia di rete EC2
			Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::EC2::NatGateway`	è contenuto in	Virtual private cloud (VPC)
		è contenuto in	Sottorete
	`AWS::EC2::EgressOnlyInternetGateway`	è collegata a	Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::EC2::EC2Fleet`	N/A	ND
	`AWS::EC2::SpotFleet`	ND	ND
	`AWS::EC2::PrefixList`	ND	ND
	`AWS::EC2::FlowLog`	ND	ND
	`AWS::EC2::TransitGateway`	ND	ND
	`AWS::EC2::TransitGatewayAttachment`	ND	ND
	`AWS::EC2::TransitGatewayRouteTable`	ND	N/A
	`AWS::EC2::VPCEndpoint`	è contenuto in	Virtual private cloud (VPC)
		è collegata a	Interfaccia di rete
		è contenuto in	Sottorete
		è contenuto in	Tabella di routing

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::EC2::VPCEndpointService`	è associata a	ElasticLoadBilanciamento V2 LoadBalancer
	`AWS::EC2::VPCPeeringConnection`	è associata a	Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::EC2::RegisteredHAInstance`	è associata a	Istanza EC2
	`AWS::EC2::SubnetRouteTableAssociation`	N/A	ND
	`AWS::EC2::LaunchTemplate`	ND	ND
	`AWS::EC2::NetworkInsightsAccessScopeAnalysis`	ND	ND
	`AWS::EC2::TrafficMirrorTarget`	ND	ND
	`AWS::EC2::TrafficMirrorSession`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::EC2::DHCPOptions`	ND	ND
	`AWS::EC2::IPAM`	ND	ND
	`AWS::EC2::NetworkInsightsPath`	ND	ND
	`AWS::EC2::TrafficMirrorFilter`	ND	ND
	`AWS::EC2::CapacityReservation`	ND	ND
	`AWS::EC2::ClientVpnEndpoint`	ND	N/A
	`AWS::EC2::CustomerGateway`	è collegata a	Connessione VPN
	`AWS::EC2::InternetGateway`	è collegata a	Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::EC2::NetworkAcl`	N/A	N/A
	`AWS::EC2::RouteTable`	contiene	Istanza EC2
			Interfaccia di rete EC2
			Sottorete

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
			Gateway VPN
		è contenuto in	Virtual private cloud (VPC)
	`AWS::EC2::Subnet`	contiene	Istanza EC2
			Interfaccia di rete EC2
		è collegata a	ACL rete
		è contenuto in	Tabella di routing
			Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::EC2::VPC`	contiene	Istanza EC2
			Interfaccia di rete EC2
			Lista di controllo degli accessi di rete
			Tabella di routing
			Sottorete
		è associata a	Gruppo di sicurezza
		è collegata a	Internet Gateway
			Gateway VPN
	`AWS::EC2::VPNConnection`	è collegata a	Gateway del cliente
			Gateway VPN

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::EC2::VPNGateway`	è collegata a	Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
			Connessione VPN
		è contenuto in	Tabella di routing
	`AWS::EC2::IPAMScope`	N/A	ND
	`AWS::EC2::CarrierGateway`	ND	ND
	`AWS::EC2::TransitGatewayConnect`	ND	ND
	`AWS::EC2::IPAMPool`	ND	ND
	`AWS::EC2::TransitGatewayMulticastDomain`	ND	ND
	`AWS::EC2::NetworkInsightsAccessScope`	ND	ND
	`AWS::EC2::NetworkInsightsAnalysis`	ND	N/A

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Elastic Block Store	`AWS::EC2::Volume`	è collegata a	Istanza EC2
EC2 Image Builder	`AWS::ImageBuilder::ImagePipeline`	N/A	ND
	`AWS::ImageBuilder::DistributionConfiguration`	ND	ND
	`AWS::ImageBuilder::ContainerRecipe`	ND	ND
	`AWS::ImageBuilder::InfrastructureConfiguration`	ND	ND
	`AWS::ImageBuilder::ImageRecipe`	ND	N/A

*AWS Config registra i dettagli di configurazione degli host dedicati e le istanze che vengono avviate su di essi. Di conseguenza, è possibile utilizzarla AWS Config come fonte di dati quando si segnala la conformità con le licenze software legate al server. Ad esempio, puoi visualizzare la cronologia della configurazione di un'istanza e determinare quale su quale AMI (Amazon Machine Image) è basata. Quindi, puoi cercare nella cronologia della configurazione dell'host, che include i dettagli come il numero di socket e core, per verificare che l'host sia conforme ai requisiti di licenza dell'AMI. Per

ulteriori informazioni, consulta Tracking Configuration Changes with AWS Config nella Amazon EC2 User Guide.

* La definizione delle SecurityGroup proprietà EC2 contiene blocchi IP CIDR, che vengono convertiti internamente in intervalli IP e possono restituire risultati imprevisti quando si cerca di trovare un intervallo IP specifico. Per soluzioni alternative nella ricerca di intervalli IP specifici, consulta Limitazioni per query avanzate.

Amazon Elastic Container Registry

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Elastic Container Registry	`AWS::ECR::Repository`	N/A	ND
	`AWS::ECR::RegistryPolicy`	ND	ND
	`AWS::ECR::PullThroughCacheRule`	ND	N/A
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	N/A	N/A

Amazon Elastic Container Service

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Elastic Container Service	`AWS::ECS::Cluster`	N/A	ND
	`AWS::ECS::TaskDefinition`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::ECS::Service` *	ND	ND
	`AWS::ECS::TaskSet`	ND	ND
	`AWS::ECS::Capacity Provider`	ND	N/A

*Questo servizio supporta attualmente solo il nuovo formato dei nomi delle risorse Amazon (ARN). Per ulteriori informazioni, consulta ID e nomi delle risorse Amazon (ARN) nella Guida per gli sviluppatori ECS.

Vecchio (non supportato): `arn:aws:ecs:`*`region`*`:`*`aws_account_id`*`:service/`*`service-name`*

Nuovo (supportato): `arn:aws:ecs:`*`region`*`:`*`aws_account_id`*`:service/`*`cluster-name`*`/`*`service-name`*

Amazon Elastic File System

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Elastic File System	`AWS::EFS::FileSystem`	N/A	ND
	`AWS::EFS::AccessPoint`	ND	N/A

Amazon Elastic Kubernetes Service

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Elastic Kubernetes Service	`AWS::EKS::Cluster`	N/A	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::EKS::FargateProfile`	ND	ND
	`AWS::EKS::IdentityProviderConfig`	ND	ND
	`AWS::EKS::Addon`	ND	N/A

Amazon EMR

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon EMR	`AWS::EMR::SecurityConfiguration`	N/A	N/A

Amazon EventBridge

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon EventBridge	`AWS::Events::EventBus`	N/A	ND
	`AWS::Events::ApiDestination`	ND	ND
	`AWS::Events::Archive`	ND	ND
	`AWS::Events::Endpoint`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::Events::Connection`	ND	ND
	`AWS::Events::Rule`	ND	N/A
EventBridge Schemi Amazon	`AWS::EventSchemas::RegistryPolicy`	N/A	ND
	`AWS::EventSchemas::Discoverer`	ND	ND
	`AWS::EventSchemas::Schema`	ND	N/A

Amazon Forecast

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Forecast	`AWS::Forecast::Dataset`	N/A	ND
	`AWS::Forecast::DatasetGroup`	ND	N/A

Amazon Fraud Detector

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Fraud Detector	`AWS::FraudDetector::Label`	N/A	ND
	`AWS::FraudDetector::EntityType`	ND	ND
	`AWS::FraudDetector::Variable`	ND	ND
	`AWS::FraudDetector::Outcome`	ND	N/A

Amazon GuardDuty

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon GuardDuty	`AWS::GuardDuty::Detector`	N/A	ND
	`AWS::GuardDuty::ThreatIntelSet`	ND	ND
	`AWS::GuardDuty::IPSet`	ND	ND
	`AWS::GuardDuty::Filter`	ND	N/A

Amazon Inspector

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Inspector	`AWS::InspectorV2::Filter`	N/A	N/A

Amazon Interactive Video Service

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Interactive Video Service	`AWS::IVS::Channel`	N/A	ND
	`AWS::IVS::RecordingConfiguration`	ND	ND
	`AWS::IVS::PlaybackKeyPair`	ND	N/A

Amazon Keyspaces (per Apache Cassandra)

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Keyspaces (per Apache Cassandra)	`AWS::Cassandra::Keyspace`	N/A	N/A

OpenSearch Servizio Amazon

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
OpenSearch Servizio Amazon	`AWS::Elasticsearch::Domain`	è associata a	Chiave KMS
			Gruppo di sicurezza EC2
			Sottorete EC2
			Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::OpenSearch::Domain`	N/A	N/A

> **Note**
>
> L'8 settembre 2021, Amazon Elasticsearch Service è stato rinominato Amazon Service. OpenSearch OpenSearch Il servizio supporta OpenSearch oltre al sistema operativo Elasticsearch legacy. Per ulteriori informazioni, consulta Amazon OpenSearch Service - Riepilogo delle modifiche.
> Puoi continuare a visualizzare i dati relativi al tipo `AWS::OpenSearch::Domain` di `AWS::Elasticsearch::Domain` risorsa esistente per diverse settimane, anche se esegui l'upgrade di uno o più domini a OpenSearch.

Amazon Personalize

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Personalize	`AWS::Personalize::Dataset`	N/A	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::Personalize::Schema`	ND	ND
	`AWS::Personalize::Solution`	ND	ND
	`AWS::Personalize::DatasetGroup`	ND	N/A

Amazon Pinpoint

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Pinpoint	`AWS::Pinpoint::ApplicationSettings`	N/A	ND
	`AWS::Pinpoint::Segment`	ND	ND
	`AWS::Pinpoint::App`	ND	ND
	`AWS::Pinpoint::Campaign`	ND	ND
	`AWS::Pinpoint::InAppTemplate`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::Pinpoint::EmailChannel`	ND	ND
	`AWS::Pinpoint::EmailTemplate`	ND	ND
	`AWS::Pinpoint::EventStream`	ND	N/A

Database Amazon Quantum Ledger (Amazon QLDB)

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon QLDB	`AWS::QLDB::Ledger`	N/A	N/A

Amazon Kendra

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Kendra	`AWS::Kendra::Index`	N/A	N/A

Amazon Kinesis

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Kinesis	`AWS::Kinesis::Stream`	N/A	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::Kinesis::StreamConsumer`	ND	N/A
Amazon Kinesis Analytics V2	`AWS::KinesisAnalyticsV2::Application`	N/A	N/A
Amazon Data Firehose	`AWS::KinesisFirehose::DeliveryStream`	N/A	N/A
Flusso video Kinesis	`AWS::KinesisVideo::SignalingChannel`	N/A	ND
	`AWS::KinesisVideo::Stream`	ND	N/A

Amazon Lex

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Lex	`AWS::Lex::BotAlias`	N/A	ND
	`AWS::Lex::Bot`	ND	N/A

Amazon Lightsail

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Lightsail	`AWS::Lightsail::Disk`	N/A	ND
	`AWS::Lightsail::Certificate`	ND	ND
	`AWS::Lightsail::Bucket`	ND	ND
	`AWS::Lightsail::StaticIp`	ND	N/A

Amazon Lookout per le metriche

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Lookout per le metriche	`AWS::LookoutMetrics::Alert`	N/A	N/A

Amazon Lookout per Vision

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Lookout per Vision	`AWS::LookoutVision::Project`	N/A	N/A

Grafana gestito da Amazon

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Grafana gestito da Amazon	`AWS::Grafana::Workspace`	N/A	N/A

Amazon Managed Service per Prometheus

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Managed Service per Prometheus	`AWS::APS::RuleGroupsNamespace`	N/A	N/A

Amazon MemoryDB per Redis

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon MemoryDB per Redis	`AWS::MemoryDB::SubnetGroup`	N/A	N/A

Amazon MQ

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon MQ	`AWS::AmazonMQ::Broker`	N/A	N/A

Amazon Managed Streaming per Apache Kafka

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Managed Streaming per Apache Kafka	`AWS::MSK::Cluster`	N/A	ND
	`AWS::MSK::Configuration`	ND	ND
	`AWS::MSK::BatchScramSecret`	ND	ND
	`AWS::MSK::ClusterPolicy`	ND	ND
	`AWS::MSK::VpcConnection`	ND	N/A
Amazon Managed Streaming per Apache Kafka Connect	`AWS::KafkaConnect::Connector`	N/A	N/A

Amazon Redshift

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Redshift	`AWS::Redshift::Cluster`	è associata a	Cluster parameter group (Gruppo di parametri del cluster)
			Gruppo di sicurezza del cluster
			Gruppo di sottoreti del cluster

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
			Gruppo di sicurezza
			Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::Redshift::ClusterParameterGroup`	N/A	ND
	`AWS::Redshift::ClusterSecurityGroup`	ND	ND
	`AWS::Redshift::ScheduledAction`	ND	N/A
	`AWS::Redshift::ClusterSnapshot`	è associata a	Cluster
			Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::Redshift::ClusterSubnetGroup`	è associata a	Sottorete
			Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::Redshift::EventSubscription`	N/A	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::Redshift::EndpointAccess`	ND	ND
	`AWS::Redshift::EndpointAuthorization`	ND	N/A

Amazon Relational Database Service

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Relational Database Service	`AWS::RDS::DBInstance`	è associata a	Gruppo di sicurezza EC2
			Gruppo di sicurezza DB RDS
			Gruppo di sottoreti RDS DB
	`AWS::RDS::DBSecurityGroup`	è associata a	Gruppo di sicurezza EC2
			Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::RDS::DBSnapshot`	è associata a	Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::RDS::DBSubnetGroup`	è associata a	Gruppo di sicurezza EC2

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
			Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::RDS::EventSubscription`	N/A	N/A
	`AWS::RDS::DBCluster`	contiene	Istanze database RDS
		è associata a	Gruppo di sottoreti RDS DB
			Gruppo di sicurezza EC2
	`AWS::RDS::DBClusterSnapshot`	è associata a	cluster DB RDS
			Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
	`AWS::RDS::GlobalCluster`	N/A	ND
	`AWS::RDS::OptionGroup`	ND	N/A

Amazon Route 53

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Route 53	`AWS::Route53::HostedZone`	N/A	ND
	`AWS::Route53::HealthCheck`	ND	ND
Amazon Route 53 Resolver	`AWS::Route53Resolver::ResolverEndpoint`	ND	ND
	`AWS::Route53Resolver::ResolverRule`	ND	ND
	`AWS::Route53Resolver::ResolverRuleAssociation`	ND	ND
	`AWS::Route53Resolver::FirewallDomainList`	ND	ND
	`AWS::Route53Resolver::FirewallRuleGroupAssociation`	ND	ND
	`AWS::Route53Resolver::ResolverQueryLoggingConfig`	ND	ND
	`AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation`	ND	ND
	`AWS::Route53Resolver::FirewallRuleGroup`	ND	N/A
Amazon Route 53 Application Recovery Controller	`AWS::Route53RecoveryReadiness::Cell`	N/A	ND
	`AWS::Route53RecoveryReadiness::ReadinessCheck`	ND	ND
	`AWS::Route53RecoveryReadiness::RecoveryGroup`	ND	ND
	`AWS::Route53RecoveryControl::Cluster`	ND	ND
	`AWS::Route53RecoveryControl::ControlPanel`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::Route53RecoveryControl::RoutingControl`	ND	ND
	`AWS::Route53RecoveryControl::SafetyRule`	ND	ND
	`AWS::Route53RecoveryReadiness::ResourceSet`	ND	N/A

Amazon SageMaker

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon SageMaker	`AWS::SageMaker::CodeRepository`	N/A	ND
	`AWS::SageMaker::Domain`	ND	ND
	`AWS::SageMaker::AppImageConfig`	ND	ND
	`AWS::SageMaker::Image`	ND	ND
	`AWS::SageMaker::Model`	ND	ND
	`AWS::SageMaker::NotebookInstance`	ND	ND
	`AWS::SageMaker::NotebookIns`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`tanceLifecycleConfig`		
	`AWS::SageMaker::EndpointConfig`	ND	ND
	`AWS::SageMaker::Workteam`	ND	ND
	`AWS::SageMaker::FeatureGroup`	ND	N/A

Amazon Simple Email Service

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Simple Email Service	`AWS::SES::ConfigurationSet`	N/A	ND
	`AWS::SES::ContactList`	ND	ND
	`AWS::SES::Template`	ND	ND
	`AWS::SES::ReceiptFilter`	ND	ND
	`AWS::SES::ReceiptRuleSet`	ND	N/A

Amazon Simple Notification Service

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Simple Notification Service	`AWS::SNS::Topic`	N/A	N/A

Amazon Simple Queue Service

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Simple Queue Service	`AWS::SQS::Queue`	N/A	N/A

Amazon Simple Storage Service

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon Simple Storage Service	`AWS::S3::Bucket` *	N/A	ND
	`AWS::S3::AccountPublicAccessBlock`	ND	ND
	`AWS::S3::MultiRegionAccessPoint`	ND	ND
	`AWS::S3::StorageLens`	ND	ND
	`AWS::S3::AccessPoint`	ND	N/A

* Se hai configurato AWS Config la registrazione dei bucket S3 e non ricevi notifiche di modifica della configurazione, verifica che le policy dei bucket S3 dispongano delle autorizzazioni richieste. Per ulteriori informazioni, consulta Gestione delle autorizzazioni per la registrazione dei bucket S3.

Attributi del bucket Amazon S3

AWS Config registra anche i seguenti attributi per il tipo di risorsa bucket Amazon S3.

Attributes	Descrizione
AccelerateConfiguration	Accelerazione del trasferimento dei dati su grandi distanze tra il client e un bucket.
BucketAcl	Lista di controllo accessi per gestire l'accesso ai bucket e agli oggetti.
BucketPolicy	Policy che definisca le autorizzazioni per il bucket.
CrossOriginConfigurazione	Consenti richieste cross-origin al bucket.
LifecycleConfiguration	Le regole che definiscono il ciclo di vita per oggetti nel bucket.
LoggingConfiguration	La registrazione consente di tenere traccia delle richieste di accesso al bucket.
NotificationConfiguration	Notifiche di eventi usate per inviare allarmi o attivare flussi di lavoro per specifici eventi del bucket.
ReplicationConfiguration	Automatico, copia asincrona degli oggetti tra bucket in diverse regioni AWS .
RequestPaymentConfigurazione	Il pagamento a carico del richiedente è abilitato.
TaggingConfiguration	Tags aggiunti al bucket per la categorizzazione. Inoltre puoi utilizzare l'applicazione di tag per verificare la fatturazione.
WebsiteConfiguration	L'hosting di siti Web statici è abilitata per il bucket.
VersioningConfiguration	La funzione di gestione delle versioni è abilitata per il bucket.

Per ulteriori informazioni sugli attributi, consulta Opzioni di configurazione dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

Amazon WorkSpaces

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Amazon WorkSpaces	`AWS::WorkSpaces::ConnectionAlias`	N/A	ND
	`AWS::WorkSpaces::Workspace`	ND	N/A

AWS Amplify

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Amplify	`AWS::Amplify::App`	N/A	ND
	`AWS::Amplify::Branch`	ND	N/A

AWS AppConfig

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS AppConfig	`AWS::AppConfig::Application`	N/A	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::AppConfig::Environment`	ND	ND
	`AWS::AppConfig::ConfigurationProfile`	ND	ND
	`AWS::AppConfig::DeploymentStrategy`	ND	ND
	`AWS::AppConfig::HostedConfigurationVersion`	ND	ND
	`AWS::AppConfig::ExtensionAssociation`	ND	N/A

AWS App Runner

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS App Runner	`AWS::AppRunner::VpcConnector`	N/A	ND
	`AWS::AppRunner::Service`	ND	N/A

AWS App Mesh

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS App Mesh	`AWS::AppMesh::VirtualNode`	N/A	ND
	`AWS::AppMesh::VirtualService`	ND	ND
	`AWS::AppMesh::VirtualGateway`	ND	ND
	`AWS::AppMesh::VirtualRouter`	ND	ND
	`AWS::AppMesh::Route`	ND	ND
	`AWS::AppMesh::GatewayRoute`	ND	ND
	`AWS::AppMesh::Mesh`	ND	N/A

AWS AppSync

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS AppSync	`AWS::AppSync::GraphQLApi`	N/A	N/A

AWS Audit Manager

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Audit Manager	`AWS::AuditManager::Assessment`	N/A	N/A

AWS Auto Scaling

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	contiene	Istanza Amazon EC2
		è associata a	Classic Load Balancer
			Configurazione di avvio per Auto Scaling
			Sottorete
	`AWS::AutoScaling::LaunchConfiguration`	è associata a	Gruppo di sicurezza Amazon EC2
	`AWS::AutoScaling::ScalingPolicy`	è associata a	Gruppo con scalabilità automatica
			Allarme
	`AWS::AutoScaling::ScheduledAction`	è associata a	Gruppo con scalabilità automatica

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::AutoScaling::WarmPool`	N/A	N/A

AWS Backup

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Backup	`AWS::Backup::BackupPlan`	N/A	ND*
	`AWS::Backup::BackupSelection`	N/A	ND
	`AWS::Backup::BackupVault`	N/A	ND*
	`AWS::Backup::RecoveryPoint`	N/A	ND
	`AWS::Backup::ReportPlan`	ND	N/A

A causa del AWS Backup funzionamento, alcuni di questi tipi di risorse sono correlati agli altri tipi di AWS Backup risorse di questa tabella.

`AWS::Backup::BackupPlan`è correlato a `AWS::Backup::BackupSelection` dove un piano di Backup ha molte selezioni ed `AWS::Backup::BackupVault` è correlato a `AWS::Backup::RecoveryPoint` dove un AWS Backup Vault ha più punti di ripristino.

Per ulteriori informazioni, consulta Gestione dei backup tramite piani di backup e Utilizzo di vault di backup.

AWS Batch

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Batch	`AWS::Batch::JobQueue`	N/A	ND
	`AWS::Batch::ComputeEnvironment`	ND	ND
	`AWS::Batch::SchedulingPolicy`	ND	N/A

Budget AWS

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Budget AWS	`AWS::Budgets::BudgetsAction`	N/A	N/A

AWS Certificate Manager

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Certificate Manager	`AWS::ACM::Certificate`	N/A	N/A

AWS CloudFormation

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS CloudFormation	`AWS::CloudFormation::Stack` *	contiene	Tipi di AWS risorse supportati

*AWS Config registra le modifiche alla configurazione AWS CloudFormation degli stack e dei tipi di risorse supportati negli stack. AWS Config non registra le modifiche alla configurazione per i tipi di risorse nello stack che non sono ancora supportati. I tipi di risorse non supportati sono raccolti nella sezione di configurazione complementare dell'elemento di configurazione dello stack.

AWS CloudTrail

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS CloudTrail	`AWS::CloudTrail::Trail`	N/A	N/A

AWS Cloud9

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Cloud9	`AWS::Cloud9::EnvironmentEC2`	N/A	N/A

AWS Cloud Map

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Individuazione dei servizi	`AWS::ServiceDiscovery::Service`	N/A	ND
	`AWS::ServiceDiscovery::PublicDnsNamespace`	ND	ND
	`AWS::ServiceDiscovery::HttpNamespace`	ND	ND
`AWS::ServiceDiscovery::Instance`	ND	N/A	

AWS CodeArtifact

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	N/A	N/A

AWS CodeBuild

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS CodeBuild	`AWS::CodeBuild::Project` *	è associata a	Bucket S3
			Ruolo IAM
	`AWS::CodeBuild::ReportGroup`	N/A	N/A

* Per ulteriori informazioni su come AWS Config si integra con AWS CodeBuild, consulta Use AWS Config with AWS CodeBuild Sample.

AWS CodeDeploy

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS CodeDeploy	`AWS::CodeDeploy::Application`	contiene	DeploymentGroup
	`AWS::CodeDeploy::DeploymentConfig`	N/A	N/A
	`AWS::CodeDeploy::DeploymentGroup`	è contenuto in	Applicazione

AWS CodePipeline

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS CodePipeline	`AWS::CodePipeline::Pipeline` *	è collegata a	Bucket S3
		è associata a	IAM role (Ruolo IAM)
			Progetto codice
			Funzione Lambda
			Stack CloudFormation
			ElasticBeanstalk applicazione

*AWS Config registra le modifiche alla configurazione delle CodePipeline pipeline e ai tipi di risorse supportati nelle pipeline. AWS Config non registra le modifiche alla configurazione per i tipi di risorse nelle pipeline che non sono ancora supportati. I tipi di risorse non supportati come `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, e `ECS service` sono raccolti nella sezione di configurazione complementare dell'elemento di configurazione dello stack.

AWS Config

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Config	`AWS::Config::ResourceCompliance` *	è associata a	Tutte le risorse*
	`AWS::Config::ConformancePackCompliance`	N/A	ND
	`AWS::Config::Confi`	ND	N/A

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`gurationRecorder` *		

*La relazione tra `AWS::Config::ResourceCompliance` e una risorsa correlata dipende dal modo in cui `AWS::Config::ResourceCompliance` riporta la conformità per quel tipo di risorsa specifico.

* `AWS::Config::ConfigurationRecorder` è un tipo di risorsa di sistema AWS Config e la registrazione di questo tipo di risorsa è abilitata per impostazione predefinita.

> **Note**
>
> La registrazione dei tipi di risorse `AWS::Config::ConformancePackCompliance` e `AWS::Config::ConfigurationRecorder` è disponibile senza costi aggiuntivi.

AWS Database Migration Service

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Database Migration Service	`AWS::DMS::EventSubscription`	N/A	ND
	`AWS::DMS::ReplicationSubnetGroup`	ND	ND
	`AWS::DMS::ReplicationInstance`	ND	ND
	`AWS::DMS::ReplicationTask`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::DMS::Certificate`	ND	ND
	`AWS::DMS::Endpoint`	ND	N/A

AWS DataSync

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS DataSync	`AWS::DataSync::LocationSMB`	N/A	ND
	`AWS::DataSync::LocationFSxLustre`	ND	ND
	`AWS::DataSync::LocationFSxWindows`	ND	ND
	`AWS::DataSync::LocationS3`	ND	ND
	`AWS::DataSync::LocationEFS`	ND	ND
	`AWS::DataSync::LocationNFS`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::DataSync::LocationHDFS`	ND	ND
	`AWS::DataSync::LocationObjectStorage`	ND	ND
	`AWS::DataSync::Task`	ND	N/A

AWS Device Farm

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Device Farm	`AWS::DeviceFarm::TestGridProject`	N/A	ND
	`AWS::DeviceFarm::InstanceProfile`	ND	ND
	`AWS::DeviceFarm::Project`	ND	N/A

AWS Elastic Beanstalk

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Application`	contiene	Versione dell'applicazione di Elastic Beanstalk
			Ambiente di Elastic Beanstalk
		è associata a	IAM role (Ruolo IAM)
	`AWS::ElasticBeanstalk::ApplicationVersion`	è contenuto in	Applicazione Elastic Beanstalk
		è associata a	Ambiente di Elastic Beanstalk
			Bucket S3
	`AWS::ElasticBeanstalk::Environment`	è contenuto in	Applicazione Elastic Beanstalk
		è associata a	Versione dell'applicazione di Elastic Beanstalk
			Ruolo IAM
		contiene	CloudFormation Pila

AWS Fault Injection Service

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Fault Injection Service	`AWS::FIS::Experimentemplate`	N/A	N/A

AWS Global Accelerator

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	N/A	ND
	`AWS::GlobalAccelerator::EndpointGroup`	ND	ND
	`AWS::GlobalAccelerator::Accelerator`	ND	N/A

AWS Glue

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Glue	`AWS::Glue::Job`	N/A	ND
	`AWS::Glue::Classifier`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::Glue::MLTransform`	ND	N/A

AWS Ground Station

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Ground Station	`AWS::GroundStation::Config`	N/A	ND
	`AWS::GroundStation::MissionProfile`	ND	ND
	`AWS::GroundStation::DataflowEndpointGroup`	ND	N/A

AWS HealthLake

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS HealthLake	`AWS::HealthLake::FHIRDatastore`	N/A	N/A

AWS Identity and Access Management (IAM)

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Identity and Access Management	`AWS::IAM::User`	è collegata a	Gruppo IAM
			policy gestita dal cliente di IAM
	`AWS::IAM::Group`	contiene	Utente IAM
		è collegata a	policy gestita dal cliente di IAM
	`AWS::IAM::Role`	è collegata a	policy gestita dal cliente di IAM
	`AWS::IAM::Policy`	è collegata a	Utente IAM
			Gruppo IAM
			Ruolo IAM
	`AWS::IAM::SAMLProvider`	N/A	ND
	`AWS::IAM::ServerCertificate`	ND	ND
	`AWS::IAM::InstanceProfile`	ND	ND
	`AWS::IAM::OIDCProvider`	ND	ND
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	ND	N/A

AWS Config include politiche in linea con i dettagli di configurazione registrati. Per ulteriori informazioni sulle policy inline, consulta Policy gestite e policy inline nella Guida per l'utente IAM.

AWS IoT

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS IoT	`AWS::IoT::Authorizer`	N/A	ND
	`AWS::IoT::SecurityProfile`	ND	ND
	`AWS::IoT::RoleAlias`	ND	ND
	`AWS::IoT::Dimension`	ND	ND
	`AWS::IoT::Policy`	ND	ND
	`AWS::IoT::MitigationAction`	ND	ND
	`AWS::IoT::ScheduledAudit`	ND	ND
	`AWS::IoT::AccountAuditConfiguration`	ND	ND
	`AWS::IoTSiteWise::Gateway`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::IoT::CustomMetric`	ND	ND
	`AWS::IoT::JobTemplate`	ND	ND
	`AWS::IoT::ProvisioningTemplate`	ND	ND
	`AWS::IoT::CACertificate`	ND	ND
AWS IoT Wireless	`AWS::IoTWireless::ServiceProfile`	ND	ND
	`AWS::IoTWireless::MulticastGroup`	ND	ND
	`AWS::IoTWireless::FuotaTask`	ND	ND
AWS IoT Core	`AWS::IoT::FleetMetric`	ND	ND
AWS IoT Analytics	`AWS::IoTAnalytics::Datastore`	ND	ND
	`AWS::IoTAnalytics::Dataset`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::IoTAnalytics::Pipeline`	ND	ND
	`AWS::IoTAnalytics::Channel`	ND	ND
AWS IoT Events	`AWS::IoTEvents::Input`	ND	ND
	`AWS::IoTEvents::DetectorModel`	ND	ND
	`AWS::IoTEvents::AlarmModel`	ND	ND
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`	ND	ND
	`AWS::IoTTwinMaker::Entity`	ND	ND
	`AWS::IoTTwinMaker::Scene`	ND	ND
	`AWS::IoTTwinMaker::SyncJob`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS IoT SiteWise	`AWS::IoTSiteWise::Dashboard`	ND	ND
	`AWS::IoTSiteWise::Project`	ND	ND
	`AWS::IoTSiteWise::Portal`	ND	ND
	`AWS::IoTSiteWise::AssetModel`	ND	ND
AWS IoT Greengrass Version 2	`AWS::GreengrassV2::ComponentVersion`	ND	N/A

AWS Key Management Service

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Key Management Service	`AWS::KMS::Key`	N/A	ND
	`AWS::KMS::Alias`	ND	N/A

AWS Lambda

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Lambda	`AWS::Lambda::Function`	è associata a	IAM role (Ruolo IAM)
			Gruppo di sicurezza EC2
		è contenuto in	Sottorete EC2
	`AWS::Lambda::Alias`	N/A	ND
	`AWS::Lambda::CodeSigningConfig`	ND	N/A

AWS Mainframe Modernization

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Mainframe Modernization	`AWS::M2::Environment`	N/A	N/A

AWS Network Firewall

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	è collegata a	Sottorete EC2
		è associata a	NetworkFirewall FirewallPolicy
	`AWS::NetworkFirewa`	è associata a	NetworkFirewall RuleGroup

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`ll::FirewallPolicy`		
	`AWS::NetworkFirewall::RuleGroup`	N/A	ND
	`AWS::NetworkFirewall::TLSInspectionConfiguration`	ND	N/A

AWS Network Manager

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Network Manager	`AWS::NetworkManager::TransitGatewayRegistration`	N/A	ND
	`AWS::NetworkManager::Site`	ND	ND
	`AWS::NetworkManager::Device`	ND	ND
	`AWS::NetworkManager::Link`	ND	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`AWS::NetworkManager::GlobalNetwork`	ND	ND
	`AWS::NetworkManager::CustomerGatewayAssociation`	ND	ND
	`AWS::NetworkManager::LinkAssociation`	ND	ND
	`AWS::NetworkManager::ConnectPeer`	ND	N/A

AWS Panorama

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Panorama	`AWS::Panorama::Package`	N/A	N/A

AWS Private Certificate Authority

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Private Certificate Authority	`AWS::ACMPCA::Certi`	N/A	ND

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
	`ficateAuthority`		
	`AWS::ACMPCA::CertificateAuthorityActivation`	ND	N/A

AWS Resilience Hub

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Resilience Hub	`AWS::ResilienceHub::ResiliencyPolicy`	N/A	ND
	`AWS::ResilienceHub::App`	ND	N/A

Esploratore di risorse AWS

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Esploratore di risorse AWS	`AWS::ResourceExplorer2::Index`	N/A	N/A

AWS RoboMaker

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS RoboMaker	`AWS::RoboMaker::RobotApplicationVersion`	N/A	ND
	`AWS::RoboMaker::RobotApplication`	ND	ND
	`AWS::RoboMaker::SimulationApplication`	ND	N/A

AWS Signer

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Signer	`AWS::Signer::SigningProfile`	N/A	N/A

AWS Secrets Manager

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Secrets Manager	`AWS::SecretsManager::Secret`	è associata a	valida e completa
		è associata a	Chiave KMS

AWS Service Catalog

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Service Catalog	`AWS::ServiceCatalog::CloudFormationProduct`	è contenuto in	Portfolio
		è associata a	CloudFormationProvisionedProduct
	`AWS::ServiceCatalog::CloudFormationProvisionedProduct`	è associata a	Portfolio
			CloudFormationProdotto
			CloudFormationPila
	`AWS::ServiceCatalog::Portfolio`	contiene	CloudFormationProdotto

AWS Shield

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Shield	`AWS::Shield::Protection`	è associata a	CloudFront Distribuzione Amazon
	`AWS::ShieldRegional::Protection`	è associata a	EIP EC2
		è associata a	ElasticLoadBalancing Bilanciatore
		è associata a	ElasticLoadBilanciamento V2 LoadBalancer

AWS Step Functions

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Step Functions	`AWS::StepFunctions::Activity`	N/A	ND
	`AWS::StepFunctions::StateMachine`	ND	N/A

AWS Systems Manager

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Systems Manager	`AWS::SSM::ManagedInstanceInventory` *	è associata a	Istanza EC2
	`AWS::SSM::PatchCompliance`	è associata a	Inventario delle istanze gestite
	`AWS::SSM::AssociationCompliance`	è associata a	Inventario delle istanze gestite
	`AWS::SSM::FileData`	è associata a	Inventario delle istanze gestite
	`AWS::SSM::Document`	N/A	N/A

*Per ulteriori informazioni sull'inventario delle istanze gestite, consulta Recording Software Configuration for Managed Instances.

AWS Transfer Family

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Transfer Family	`AWS::Transfer::Agreement`	N/A	ND
	`AWS::Transfer::Connector`	ND	ND
	`AWS::Transfer::Workflow`	ND	ND
	`AWS::Transfer::Certificate`	ND	ND
	`AWS::Transfer::Profile`	ND	N/A

AWS WAF

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS WAF	`AWS::WAF::RateBasedRule`	N/A	ND
	`AWS::WAF::Rule`	ND	N/A
	`AWS::WAF::WebACL`	è associata a	Regola WAF
			Regola basata sulla frequenza WAF

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
			WAF Rulegroup
	`AWS::WAF::RuleGroup`	è associata a	Regola WAF
	`AWS::WAFRegional::RateBasedRule`	N/A	ND
	`AWS::WAFRegional::Rule`	ND	N/A
	`AWS::WAFRegional::WebACL`	è associata a	ElasticLoadBilanciamento V2 LoadBalancer
			Regola WAFRegional
			Regola basata sull'intensità del flusso di WAFRegional
			WAFRegional Rulegroup
	`AWS::WAFRegional::RuleGroup`	è associata a	Regola WAFRegional
AWS WAF V2	`AWS::WAFv2::WebACL`	è associata a	ElasticLoadBilanciamento V2 LoadBalancer
			ApiGateway Fase
			WAFv2 IPSet

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
			WAFv2 RegexPatternSet
			WAFv2 RuleGroup
			WAFv2 ManagedRuleSet
	`AWS::WAFv2::RuleGroup`	è associata a	WAFv2 IPSet
			WAFv2 RegexPatternSet
	`AWS::WAFv2::ManagedRuleSet`	è associata a	WAFv2 RuleGroup
	`AWS::WAFv2::IPSet`	N/A	ND
	`AWS::WAFv2::RegexPatternSet`	ND	N/A

AWS X-Ray

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS X-Ray	`AWS::XRay::EncryptionConfig`	N/A	N/A

Sistema di bilanciamento del carico elastico

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
Sistema di bilanciamento del carico elastico	Application Load Balancer `AWS::ElasticLoadBalancingV2::LoadBalancer`	è associata a	Gruppo di sicurezza EC2
		è collegata a	Sottorete
		è contenuto in	Virtual private cloud (VPC)
	Ascoltatore Application Load Balancer `AWS::ElasticLoadBalancingV2::Listener`	N/A	N/A
	Classic Load Balancer `AWS::ElasticLoadBalancing::LoadBalancer`	è associata a	Gruppo di sicurezza EC2
		è collegata a	Sottorete
		è contenuto in	Virtual private cloud (VPC)
	Network Load Balancer `AWS::ElasticLoadBalancingV2::LoadBalancer`	N/A	N/A

AWS Elemental MediaConnect

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Elemental MediaConnect	`AWS::MediaConnect::FlowEntitlement`	N/A	ND
	`AWS::MediaConnect::FlowVpcInterface`	ND	ND
	`AWS::MediaConnect::FlowSource`	ND	N/A

AWS Elemental MediaPackage

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Elemental MediaPackage	`AWS::MediaPackage::PackagingGroup`	N/A	ND
	`AWS::MediaPackage::PackagingConfiguration`	ND	N/A

AWS Elemental MediaTailor

AWS Servizio	Valore tipo di risorsa	Relazione	Risorsa correlata
AWS Elemental MediaTailor	`AWS::MediaTailor::PlaybackConfiguration`	N/A	N/A

Copertura delle risorse in base alla disponibilità nelle regioni

Regioni del Nord e del Sud America

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::ACM::Certificate	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ACMPCA::CertificateAuthority	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ACMPCA::CertificateAuthorityAttivazione	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::APS::RuleGroupsNamespace	Sì	Sì	Sì	Sì	No	No	No
AWS::AccessAnalyzer::Analyzer	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AmazonMQ::Broker	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Amplify::App	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Amplify::Branch	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ApiGateway::RestApi	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::ApiGateway::Stage	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ApiGatewayV2::Api	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ApiGatewayV2::Stage	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AppConfig::Application	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AppConfig::ConfigurationProfile	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AppConfig::DeploymentStrategy	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::AppConfig::Environment	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AppConfig::ExtensionAssociation	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AppConfig::HostedConfigurationVersione	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AppFlow::Flow	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AppIntegrations::EventIntegration	No	No	Sì	Sì	No	Sì	No
AWS::AppMesh::GatewayRoute	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::AppMesh::Mesh	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AppMesh::Route	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AppMesh::VirtualGateway	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AppMesh::VirtualNode	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AppMesh::VirtualRouter	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AppMesh::VirtualService	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::AppRunner::Service	Sì	No	Sì	Sì	No	No	No
AWS::AppRunner::VpcConnector	Sì	No	Sì	Sì	No	No	No
AWS::AppStream::Application	Sì	Sì	Sì	Sì	No	Sì	No
AWS::AppStream::DirectoryConfig	Sì	Sì	Sì	Sì	No	Sì	No
AWS::AppStream::Fleet	Sì	No	Sì	Sì	No	Sì	No
AWS::AppStream::Stack	Sì	No	Sì	Sì	No	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::AppSync::GraphQLAPI	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Athena::DataCatalog	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Athena::PreparedStatement	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Athena::WorkGroup	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::AuditManager::Assessment	Sì	No	Sì	Sì	Sì	Sì	No
AWS::AutoScaling::AutoScalingGruppo	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::AutoScaling::LaunchConfiguration	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AutoScaling::ScalingPolicy	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AutoScaling::ScheduledAction	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AutoScaling::WarmPool	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Backup::BackupPlan	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Backup::BackupSelection	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Backup::BackupVault	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Backup::RecoveryPoint	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Backup::ReportPlan	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Batch::ComputeEnvironment	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Batch::JobQueue	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Batch::SchedulingPolicy	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Budgets::BudgetsAction	No	No	Sì	No	No	No	No
AWS::Cassandra::Keyspace	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Cloud9::EnvironmentEC2	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::CloudFormation::Stack	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::CloudFront::Distribution	No	No	Sì	No	No	No	No
AWS::CloudFront::StreamingDistribution	No	No	Sì	No	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::CloudTrail::Trail	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::CloudWatch::Alarm	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::CloudWatch::MetricStream	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::CodeArtifact::Repository	Sì	No	Sì	Sì	No	No	No
AWS::CodeBuild::Project	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::CodeBuild::ReportGroup	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::CodeDeploy::Application	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::CodeDeploy::DeploymentConfig	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::CodeDeploy::DeploymentGroup	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::CodeGuruProfiler::ProfilingGroup	Sì	No	Sì	Sì	No	No	No
AWS::CodeGuruReviewer::RepositoryAssociation	Sì	No	Sì	Sì	No	No	No
AWS::CodePipeline::Pipeline	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Cognito::UserPool	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Cognito::UserPoolCliente	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Cognito::User PoolGruppo	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Config::Configurationrecorder	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Config::ConformancePackConformità	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Config::ResourceCompliance	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Connect::Instance	No	No	Sì	Sì	No	Sì	No
AWS::Connect::PhoneNumber	No	No	Sì	Sì	No	Sì	No
AWS::Connect::QuickConnect	No	No	Sì	Sì	No	Sì	No
AWS::CustomerProfiles::Domain	No	No	Sì	Sì	No	Sì	No
AWS::CustomerProfiles::ObjectType	No	No	Sì	Sì	No	Sì	No
AWS::DMS::Certificate	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::DMS::Endpoint	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::DMS::EventSubscription	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::DMS::ReplicationInstance	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::DMS::ReplicationSubnetGruppo	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::DMS::ReplicationTask	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::DataSync::LocationEFS	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::DataSync::LocationF SxLustre	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::DataSync::LocationF SxWindows	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::DataSync::LocationHDFS	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::DataSync::LocationNFS	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::DataSync::LocationObjectArchiviazione	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::DataSync::LocationS3	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::DataSync::LocationSMB	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::DataSync::Task	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Detective::Graph	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::DeviceFarm::InstanceProfile	No	No	No	Sì	No	No	No
AWS::DeviceFarm::Project	No	No	No	Sì	No	No	No
AWS::DeviceFarm::TestGridProgetto	No	No	No	Sì	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::DynamoDB::Table	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::Capacity Reservation	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::CarrierGateway	Sì	No	Sì	Sì	No	Sì	No
AWS::EC2::ClientVpnPunto finale	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::CustomerGateway	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::DHCPOptions	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::EC2::EC2Fleet	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::EIP	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::EgressOnlyInternetGateway	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::FlowLog	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::Host	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::IPAM	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::EC2::IPAMPool	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::IPAMScope	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::Instance	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::InternetGateway	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::LaunchTemplate	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::NatGateway	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::EC2::NetworkAcl	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::NetworkInsightsAccessScope	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::NetworkInsightsAccessScopeAnalisi	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::NetworkInsightsAnalisi	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::NetworkInsightsPercorso	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::NetworkInterface	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::EC2::PrefixList	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::RegisteredHain Stance	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::RouteTable	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::SecurityGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::SpotFleet	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::Subnet	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::EC2::SubnetRouteTableAssociation	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::TrafficMirrorFiltro	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::TrafficMirrorSessione	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::TrafficMirrorObiettivo	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::TransitGateway	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::TransitGatewayAllegato	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::EC2::TransitGatewayConnect	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::TransitGatewayMulticastDomain	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::TransitGatewayRouteTable	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EC2::VPC	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::VPCEndpoint	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS: :EC2: :VPC EndpointService	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS: :EC2: :VPC PeeringConnection	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::VPNConnection	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::VPNGateway	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::Volume	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECR::PublicRepository	No	No	Sì	No	No	No	No
AWS::ECR::PullThroughCacheRule	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::ECR::RegistryPolicy	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ECR::Repository	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ECS::CapacityProvider	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ECS::Cluster	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECS::Service	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECS::TaskDefinition	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::ECS::TaskSet	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EFS::AccessPoint	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EFS::FileSystem	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EKS::Addon	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EKS::Cluster	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EKS::FargateProfile	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::EKS::IdentityProviderConfig	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EMR::SecurityConfiguration	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ElasticBeanstalk::Application	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ElasticBeanstalk::ApplicationVersion	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ElasticBeanstalk::Environment	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ElasticLoadBalancing::LoadBalancer	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::ElasticLoadBalancingV2::Listener	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ElasticLoadBalancingV2::LoadBalancer	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Elasticsearch::Domain	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EventSchemas::Discoverer	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EventSchemas::Registry	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::EventSchemas::RegistryPolicy	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::EventSchemas::Schema	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Events::ApiDestination	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Events::Archive	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Events::Connection	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Events::Endpoint	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Events::EventBus	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Events::Rule	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Evidently::Launch	Sì	No	Sì	Sì	No	No	No
AWS::Evidently::Project	Sì	No	Sì	Sì	No	No	No
AWS::Evidently::Segment	Sì	No	Sì	Sì	No	No	No
AWS::FIS::ExperimentTemplate	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Forecast::Dataset	Sì	No	Sì	Sì	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Forecast::DatasetGroup	Sì	No	Sì	Sì	No	No	No
AWS::FraudDetector::EntityType	Sì	No	Sì	Sì	No	No	No
AWS::FraudDetector::Label	Sì	No	Sì	Sì	No	No	No
AWS::FraudDetector::Outcome	Sì	No	Sì	Sì	No	No	No
AWS::FraudDetector::Variable	Sì	No	Sì	Sì	No	No	No
AWS::GlobalAccelerator::Accelerator	No	No	No	Sì	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::GlobalAccelerator::EndpointGroup	No	No	No	Sì	No	No	No
AWS::GlobalAccelerator::Listener	No	No	No	Sì	No	No	No
AWS::Glue::Classifier	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Glue::Job	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Glue:: MLTransform	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Grafana::Workspace	Sì	No	Sì	Sì	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::GreengrassV2::ComponentVersion	Sì	No	Sì	Sì	No	Sì	No
AWS::GroundStation::Config	Sì	Sì	Sì	Sì	No	No	No
AWS::GroundStation::DataflowEndpointGruppo	Sì	Sì	Sì	Sì	No	No	No
AWS::GroundStation::MissionProfile	Sì	Sì	Sì	Sì	No	No	No
AWS::GuardDuty::Detector	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::GuardDuty::Filter	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::GuardDovere: :IPSet	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::GuardDuty::ThreatIntelImpostare	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::HealthLake:: FHIRData Store	Sì	No	Sì	Sì	No	No	No
AWS::IAM::Group	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::IAM::InstanceProfile	No	No	Sì	No	No	No	No
AWS::IAM::OIDCProvider	No	No	Sì	No	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::IAM::Policy	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::IAM::Role	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::IAM::SAMLProvider	No	No	Sì	No	No	No	No
AWS::IAM::ServerCertificate	No	No	Sì	No	No	No	No
AWS::IAM::User	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::IVS::Channel	No	No	Sì	Sì	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::IVS::PlaybackKeyCoppia	No	No	Sì	Sì	No	No	No
AWS::IVS::RecordingConfiguration	No	No	Sì	Sì	No	No	No
AWS::ImageBuilder::ContainerRecipe	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ImageBuilder::DistributionConfiguration	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ImageBuilder::ImagePipeline	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ImageBuilder::ImageRecipe	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::ImageBuilder::InfrastructureConfiguration	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::InspectorV2::Filter	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::IoT::AccountAuditConfigurazione	Sì	No	Sì	Sì	Sì	Sì	No
AWS::IoT::Authorizer	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::IoCertificato T: :CA	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::IoT::CustomMetric	Sì	No	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::IoT::Dimension	Sì	No	Sì	Sì	Sì	Sì	No
AWS::IoT::FleetMetric	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::IoT::JobTemplate	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::IoT::MitigationAction	Sì	No	Sì	Sì	Sì	Sì	No
AWS::IoT::Policy	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::IoT::ProvisioningTemplate	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::IoT::RoleAlias	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::IoT::ScheduledAudit	Sì	No	Sì	Sì	Sì	Sì	No
AWS::IoT::SecurityProfile	Sì	No	Sì	Sì	Sì	Sì	No
AWS::IoTAnalytics::Channel	Sì	No	Sì	Sì	No	No	No
AWS::IoTAnalytics::Dataset	Sì	No	Sì	Sì	No	No	No
AWS::IoTAnalytics::Datastore	Sì	No	Sì	Sì	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::IoTAnalytics::Pipeline	Sì	No	Sì	Sì	No	No	No
AWS::IoTEvents::AlarmModel	Sì	No	Sì	Sì	No	Sì	No
AWS::IoTEvents::DetectorModel	Sì	No	Sì	Sì	No	Sì	No
AWS::IoTEvents::Input	Sì	No	Sì	Sì	No	Sì	No
AWS::IoTSiteWise::AssetModel	Sì	No	Sì	Sì	No	Sì	No
AWS::IoTSiteWise::Dashboard	Sì	No	Sì	Sì	No	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::IoTSiteWise::Gateway	Sì	No	Sì	Sì	No	Sì	No
AWS::IoTSiteWise::Portal	Sì	No	Sì	Sì	No	Sì	No
AWS::IoTSiteWise::Project	Sì	No	Sì	Sì	No	Sì	No
AWS::IoTTwinMaker::ComponentType	No	No	Sì	Sì	No	No	No
AWS::IoTTwinMaker::Entity	No	No	Sì	Sì	No	No	No
AWS::IoTTwinMaker::Scene	No	No	Sì	Sì	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::IoTTwinMaker::SyncJob	No	No	Sì	Sì	No	No	No
AWS::IoTTwinMaker::Workspace	No	No	Sì	Sì	No	No	No
AWS::IoTWireless::FuotaTask	No	Sì	Sì	Sì	No	No	No
AWS::IoTWireless::MulticastGroup	No	Sì	Sì	Sì	No	No	No
AWS::IoTWireless::ServiceProfile	No	Sì	Sì	Sì	No	No	No
AWS::KMS::Alias	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::KMS::Key	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::KafkaConnect::Connector	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Kendra::Index	Sì	No	Sì	Sì	No	Sì	No
AWS::Kinesis::Stream	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Kinesis::StreamConsumer	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::KinesisAnalyticsV2::Application	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::KinesisFirehose::DeliveryStream	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::KinesisVideo::SignalingChannel	Sì	Sì	Sì	Sì	No	Sì	No
AWS::KinesisVideo::Stream	Sì	Sì	Sì	Sì	No	Sì	No
AWS::Lambda::CodeSigningConfig	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Lambda::Function	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Lex::Bot	No	No	Sì	Sì	No	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Lex::BotAlias	No	No	Sì	Sì	No	Sì	No
AWS::Lightsail::Bucket	Sì	No	Sì	Sì	No	Sì	No
AWS::Lightsail::Certificate	Sì	No	Sì	Sì	No	Sì	No
AWS::Lightsail::Disk	Sì	No	Sì	Sì	No	Sì	No
AWS::Lightsail::StaticIp	Sì	No	Sì	Sì	No	Sì	No
AWS::Logs::Destination	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::LookoutMetrics::Alert	Sì	No	Sì	Sì	No	No	No
AWS::LookoutVision::Project	Sì	No	Sì	Sì	No	No	No
AWS::M2::Environment	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::MSK::BatchScramSegreto	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::MSK::Cluster	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::MSK::ClusterPolicy	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::MSK::Configuration	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::MSK::VpcConnection	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::MediaConnect::FlowEntitlement	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::MediaConnect::FlowSource	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::MediaConnect::FlowVpcInterfaccia	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::MediaPackage::PackagingConfiguration	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::MediaPackage::PackagingGroup	Sì	Sì	Sì	Sì	Sì	No	No
AWS::MediaTailor::PlaybackConfiguration	Sì	No	Sì	Sì	No	No	No
AWS::MemoryDB::SubnetGroup	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::NetworkFirewall::Firewall	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::NetworkFirewall::FirewallPolicy	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::NetworkFirewall::RuleGroup	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::NetworkFirewall: :TLS InspectionConfiguration	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::NetworkManager::ConnectPeer	No	No	No	Sì	No	No	No
AWS::NetworkManager::CustomerGatewayAssociazione	No	No	No	Sì	No	No	No
AWS::NetworkManager::Device	No	No	No	Sì	No	No	No
AWS::NetworkManager::GlobalNetwork	No	No	No	Sì	No	No	No
AWS::NetworkManager::Link	No	No	No	Sì	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::NetworkManager::LinkAssociation	No	No	No	Sì	No	No	No
AWS::NetworkManager::Site	No	No	No	Sì	No	No	No
AWS::NetworkManager::TransitGatewayRegistrazione	No	No	No	Sì	No	No	No
AWS::OpenSearch::Domain	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Panorama::Package	No	No	Sì	Sì	No	Sì	No
AWS::Personalize::Dataset	Sì	No	Sì	Sì	No	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Personalize::DatasetGroup	Sì	No	Sì	Sì	No	Sì	No
AWS::Personalize::Schema	Sì	No	Sì	Sì	No	Sì	No
AWS::Personalize::Solution	Sì	No	Sì	Sì	No	Sì	No
AWS::Pinpoint::App	No	No	Sì	Sì	No	Sì	No
AWS::Pinpoint::ApplicationSettings	No	No	Sì	Sì	No	Sì	No
AWS::Pinpoint::Campaign	No	No	Sì	Sì	No	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Pinpoint::EmailChannel	No	No	Sì	Sì	No	Sì	No
AWS::Pinpoint::EmailTemplate	No	No	Sì	Sì	No	Sì	No
AWS::Pinpoint::EventStream	No	No	Sì	Sì	No	Sì	No
AWS::Pinpoint::InAppModello	Sì	No	Sì	Sì	No	Sì	No
AWS::Pinpoint::Segment	No	No	Sì	Sì	No	Sì	No
AWS::QLDB::Ledger	Sì	No	Sì	Sì	No	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::QuickSight::DataSource	Sì	Sì	Sì	Sì	No	Sì	No
AWS::QuickSight::Template	Sì	Sì	Sì	Sì	No	Sì	No
AWS::QuickSight::Theme	Sì	Sì	Sì	Sì	No	Sì	No
AWS::RDS::DBCluster	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS: :RDS: :DB ClusterSnapshot	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RDS::DBInstance	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS: :RDS: :DB SecurityGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RDS::DBSnapshot	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS: :RDS: :DB SubnetGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RDS::EventSubscription	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RDS::GlobalCluster	Sì	No	Sì	Sì	Sì	Sì	No
AWS::RDS::OptionGroup	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::RUM::AppMonitor	Sì	No	Sì	Sì	No	No	No
AWS::Redshift::Cluster	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::ClusterParameterGruppo	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::ClusterSecurityGruppo	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::ClusterSnapshot	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::ClusterSubnetGruppo	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Redshift::EndpointAccess	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Redshift::EndpointAuthorization	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Redshift::EventSubscription	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::ScheduledAction	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ResilienceHub::App	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ResilienceHub::ResiliencyPolicy	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::ResourceExplorer2::Index	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::RoboMaker::RobotApplication	Sì	No	Sì	Sì	No	No	No
AWS::RoboMaker::RobotApplicationVersione	Sì	No	Sì	Sì	No	No	No
AWS::RoboMaker::SimulationApplication	Sì	No	Sì	Sì	No	No	No
AWS::Route53::HealthCheck	No	No	Sì	No	No	No	No
AWS::Route53::HostedZone	No	No	Sì	No	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Route53RecoveryControl::Cluster	No	No	No	Sì	No	No	No
AWS::Route53RecoveryControl::ControlPanel	No	No	No	Sì	No	No	No
AWS::Route53RecoveryControl::RoutingControl	No	No	No	Sì	No	No	No
AWS::Route53RecoveryControl::SafetyRule	No	No	No	Sì	No	No	No
AWS::Route53RecoveryReadiness::Cell	No	No	No	Sì	No	No	No
AWS::Route53RecoveryReadiness::ReadinessCheck	No	No	No	Sì	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Route53RecoveryReadiness::RecoveryGroup	No	No	No	Sì	No	No	No
AWS::Route53RecoveryReadiness::ResourceSet	No	No	No	Sì	No	No	No
AWS::Route53Resolver::FirewallDomainElenco	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Route53Resolver::FirewallRuleGruppo	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Route53Resolver::ResolverEndpoint	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociazione	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Route53Resolver::ResolverRule	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Route53Resolver::ResolverRuleAssociazione	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::S3::AccessPoint	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::S3::AccountPublicAccessBlock	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::S3::Bucket	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::S3::MultiRegionAccessPoint	No	No	No	Sì	No	No	No
AWS::S3::StorageLens	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SES::ConfigurationSet	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SES::ContactList	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SES::ReceiptFilter	No	No	Sì	Sì	No	No	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::SES::ReceiptRuleImpostare	No	No	Sì	Sì	No	No	No
AWS::SES::Template	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SNS::Topic	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::SQS::Queue	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SSM::AssociationCompliance	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SSM::Document	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::SSM::FileData	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SSM::ManagedInstanceInventario	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SSM::PatchCompliance	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SageMaker::AppImageConfig	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SageMaker::CodeRepository	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SageMaker::Domain	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::SageMaker::EndpointConfig	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SageMaker::FeatureGroup	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SageMaker::Image	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SageMaker::Model	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SageMaker::NotebookInstance	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::SageMaker::Workteam	Sì	No	Sì	Sì	No	Sì	No
AWS::SecretsManager::Secret	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ServiceCatalog::CloudFormationProdotto	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ServiceCatalog::Portfolio	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ServiceDiscovery::HttpNamespace	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::ServiceDiscovery::Instance	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ServiceDiscovery::PublicDnsNamespace	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::ServiceDiscovery::Service	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Shield::Protection	No	No	Sì	No	No	No	No
AWS::ShieldRegional::Protection	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Signer::SigningProfile	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::StepFunctions::Activity	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::StepFunctions::StateMachine	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Transfer::Agreement	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Transfer::Certificate	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Transfer::Connector	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::Transfer::Profile	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::Transfer::Workflow	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::WAF::RateBasedRegola	No	No	Sì	No	No	No	No
AWS::WAF::Rule	No	No	Sì	No	No	No	No
AWS::WAF::RuleGroup	No	No	Sì	No	No	No	No
AWS::WAF::WebACL	No	No	Sì	No	No	No	No
AWS::WAFRegional::RateBasedRegola	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::WAFRegional::Rule	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::WAFRegional::RuleGroup	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::WAFRegional::WebACL	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::WAFv2::IPSet	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::WAFv2::ManagedRuleImpostare	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::WAFv2::RegexPatternImpostare	Sì	Sì	Sì	Sì	Sì	Sì	No

Tipo di risorsa	Stati Uniti occidentali (California settentrionale)	Stati Uniti orientali (Virginia settentrionale)	Stati Uniti occidentali (Oregon)	Stati Uniti orientali (Ohio)	Canada occidentale (Calgary)	Canada (Centrale)	Sud America (San Paolo)
AWS::WAFv2::RuleGroup	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::WAFv2::WebACL	Sì	Sì	Sì	Sì	Sì	Sì	No
AWS::WorkSpaces::ConnectionAlias	No	Sì	Sì	Sì	No	Sì	No
AWS::WorkSpaces::Workspace	No	Sì	Sì	Sì	No	Sì	No
AWS::XRay::EncryptionConfig	Sì	Sì	Sì	Sì	Sì	Sì	No

Regioni dell'Europa

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::ACM::Certificate	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ACMPCA::CertificateAuthority	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ACMPCA::CertificateAuthorityAttivazione	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::APS::RuleGroupsNamespace	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::AccessAnalyzer::Analyzer	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AmazonMQ::Broker	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Amplify::App	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Amplify::Branch	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::ApiGateway::RestApi	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ApiGateway::Stage	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ApiGatewayV2::Api	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ApiGatewayV2::Stage	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AppConfig::Application	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::AppConfig::ConfigurationProfile	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::AppConfig::DeploymentStrategy	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::AppConfig::Environment	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::AppConfig::ExtensionAssociation	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AppConfig::HostedConfigurationVersione	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::AppFlow::Flow	No	Sì	Sì	Sì	Sì	No	No	No
AWS::AppIntegrations::EventIntegration	No	No	No	Sì	Sì	No	No	No
AWS::AppMesh::GatewayRoute	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::AppMesh::Mesh	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::AppMesh::Route	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::AppMesh::VirtualGateway	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::AppMesh::VirtualNode	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::AppMesh::VirtualRouter	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::AppMesh::VirtualService	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::AppRunner::Service	No	No	Sì	Sì	No	No	No	No
AWS::AppRunner::VpcConnector	No	No	Sì	No	No	No	No	No
AWS::AppStream::Application	No	No	Sì	Sì	Sì	No	No	No
AWS::AppStream::DirectoryConfig	No	No	Sì	Sì	Sì	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::AppStream::Fleet	No	No	Sì	Sì	Sì	No	No	No
AWS::AppStream::Stack	No	No	Sì	Sì	Sì	No	No	No
AWS::AppS ync::GraphQLAPI	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Athena::DataCatalog	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Athena::Prepa redStatement	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::Athena::WorkGroup	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::AuditManager: :Assessment	No	No	Sì	Sì	Sì	No	No	No
AWS::AutoScaling:: AutoScalingGruppo	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::AutoScaling::LaunchConfiguration	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AutoScaling::ScalingPolicy	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AutoScaling::ScheduledAction	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Auto Scaling::WarmPool	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Backup::BackupPlan	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Backup::BackupSelection	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Backup::BackupVault	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Backup::RecoveryPoint	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Backup::ReportPlan	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Batch::ComputeEnvironment	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Batch::JobQueue	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Batch::SchedulingPolicy	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Cassandra::Keyspace	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::Cloud9::EnvironmentEC2	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::CloudFormation::Stack	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::CloudTrail::Trail	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::CloudWatch::Alarm	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::CloudWatch::M etricStream	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Code Artifact::Repository	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::CodeBuild::Project	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Code Build::ReportGroup	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Code Deploy::Application	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::CodeDeploy::D eploymentConfig	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::CodeDeploy::D eploymentGroup	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::CodeGuruProfiler::ProfilingGroup	Sì	No	Sì	Sì	Sì	No	No	No
AWS::CodeGuruReviewer::RepositoryAssociation	Sì	No	Sì	Sì	Sì	No	No	No
AWS::CodePipeline::Pipeline	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Cognito::UserPool	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Cognito::UserPoolCliente	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Cognito::UserPoolGruppo	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Config::ConfigurationRecorder	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Config::ConformancePackConformità	Sì	Sì	Sì	Sì	Sì	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Config::Resou rceCompliance	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Connect::Instance	No	No	No	Sì	Sì	No	No	No
AWS::Conn ect::PhoneNumber	No	No	No	Sì	Sì	No	No	No
AWS::Conn ect::QuickConnect	No	No	No	Sì	Sì	No	No	No
AWS::CustomerProfi les::Domain	No	No	No	Sì	Sì	No	No	No
AWS::CustomerProfi les::ObjectType	No	No	No	Sì	Sì	No	No	No
AWS::DMS::Certificate	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::DMS::Endpoint	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::DMS: :EventSubscription	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::DMS: :ReplicationInstance	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::DMS::Replicat ionSubnetGruppo	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::DMS: :ReplicationTask	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Data Sync::LocationEFS	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::DataSync::Loc ationF SxLustre	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::DataSync::Loc ationF SxWindows	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Data Sync::LocationHDFS	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Data Sync::LocationNFS	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::DataSync::Loc ationObjectArchiviazione	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Data Sync::LocationS3	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Data Sync::LocationSMB	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::DataSync::Task	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Detective::Graph	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::DynamoDB::Table	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::Capacity Reservation	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::EC2::CarrierGateway	No	Sì	Sì	Sì	Sì	No	No	No
AWS::EC2::ClientVpnPunto finale	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::EC2::CustomerGateway	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::DHCPOptions	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::EC2Fleet	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::EIP	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::EgressOnlyInternetGateway	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì
AWS::EC2::FlowLog	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::EC2::Host	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::IPAM	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::IPAMPool	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::IPAMScope	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::Instance	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2: :InternetGateway	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2: :LaunchTemplate	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::EC2::NatGateway	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::EC2::NetworkAcl	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::NetworkI nsightsAccessScope	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::EC2::NetworkI nsightsAccessScopeAnalisi	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::EC2::NetworkI nsightsAnalisi	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::EC2::NetworkI nsightsPercorso	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::EC2: :NetworkInterface	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::PrefixList	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::Register edHain Stance	Sì	Sì	Sì	Sì	Sì	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::EC2::RouteTable	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::SecurityGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::SpotFleet	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::Subnet	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::SubnetRo uteTableAssociation	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2: :TrafficMirrorFiltro	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::EC2::TrafficM irrorSessione	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::EC2::TrafficM irrorObiettivo	Sì	Sì	Sì	Sì	Sì	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::EC2::TransitGateway	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::TransitGatewayAllegato	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::TransitGatewayConnect	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::EC2::TransitGatewayMulticastDomain	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::TransitGatewayRouteTable	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì
AWS::EC2::VPC	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::VPCEndpoint	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS: :EC2: :VPC EndpointService	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS: :EC2: :VPC PeeringConnection	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2: :VPNConnection	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::VPNGateway	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::Volume	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECR::PullThroughCacheRule	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECR::RegistryPolicy	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECR::Repository	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECS: :CapacityProvider	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::ECS::Cluster	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECS::Service	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECS::TaskDefinition	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECS::TaskSet	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EFS::AccessPoint	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EFS::FileSystem	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EKS::Addon	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EKS::Cluster	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::EKS::FargateProfile	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EKS::Identity ProviderConfig	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EMR::Security Configuration	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ElasticBeanst alk::Application	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::ElasticBeanst alk::ApplicationVersion	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::ElasticBeanst alk::Environment	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::ElasticLoadBa lancing::LoadBalancer	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ElasticLoadBa lancingV2::Listener	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::ElasticLoadBalancingV2::LoadBalancer	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Elasticsearch::Domain	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EventSchemas::Discoverer	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::EventSchemas::Registry	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::EventSchemas::RegistryPolicy	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::EventSchemas::Schema	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::Events::ApiDestination	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Events::Archive	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Events::Connection	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Events::Endpoint	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::Events::EventBus	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Events::Rule	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Evidently::Launch	Sì	No	Sì	Sì	No	No	No	No
AWS::Evidently::Project	Sì	No	Sì	Sì	No	No	No	No
AWS::Evidently::Segment	Sì	No	Sì	Sì	No	No	No	No
AWS::FIS::Experime ntTemplate	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Forecast::Dataset	No	No	Sì	Sì	No	No	No	No
AWS::Forecast::DatasetGroup	No	No	Sì	Sì	No	No	No	No
AWS::FraudDetector::EntityType	No	No	Sì	No	No	No	No	No
AWS::FraudDetector::Label	No	No	Sì	No	No	No	No	No
AWS::FraudDetector::Outcome	No	No	Sì	No	No	No	No	No
AWS::FraudDetector::Variable	No	No	Sì	No	No	No	No	No
AWS::Glue::Classifier	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Glue::Job	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Glue:: MLTransform	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Grafana::Workspace	No	No	Sì	Sì	Sì	No	No	No
AWS::GreengrassV2: :ComponentVersion	No	No	Sì	Sì	Sì	No	No	No
AWS::Grou ndStation::Config	Sì	No	Sì	Sì	No	No	No	No
AWS::GroundStation ::DataflowEndpointGruppo	Sì	No	Sì	Sì	No	No	No	No
AWS::GroundStation ::MissionProfile	Sì	No	Sì	Sì	No	No	No	No
AWS::GuardDuty::Detector	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::GuardDuty::Filter	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::GuardDovere: :IPSet	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::GuardDuty::Th reatIntelImpostare	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::IAM::Group	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::IAM::Policy	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::IAM::Role	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::IAM::User	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::IVS::Channel	No	No	Sì	Sì	No	No	No	No
AWS::IVS::Playback KeyCoppia	No	No	Sì	Sì	No	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::IVS::RecordingConfiguration	No	No	Sì	Sì	No	No	No	No
AWS::ImageBuilder::ContainerRecipe	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ImageBuilder::DistributionConfiguration	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::ImageBuilder::ImagePipeline	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ImageBuilder::ImageRecipe	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::ImageBuilder::InfrastructureConfiguration	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::InspectorV2::Filter	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::IoT::AccountAuditConfigurazione	Sì	Sì	Sì	Sì	Sì	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::IoT::Authorizer	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::IoCertificato T: :CA	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::IoT::CustomMetric	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::IoT::Dimension	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::IoT::FleetMetric	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::IoT::JobTemplate	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::IoT::MitigationAction	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::IoT::Policy	Sì	Sì	Sì	Sì	Sì	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::IoT::Provisio ningTemplate	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::IoT::RoleAlias	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::IoT::ScheduledAudit	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::IoT::SecurityProfile	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::IoTA nalytics::Channel	No	No	Sì	Sì	No	No	No	No
AWS::IoTAnalytics::Dataset	No	No	Sì	Sì	No	No	No	No
AWS::IoTA nalytics::Datastore	No	No	Sì	Sì	No	No	No	No
AWS::IoTAnalytics::Pipeline	No	No	Sì	Sì	No	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::IoTE vents::AlarmModel	No	No	Sì	Sì	Sì	No	No	No
AWS::IoTEvents::De tectorModel	No	No	Sì	Sì	Sì	No	No	No
AWS::IoTEvents::Input	No	No	Sì	Sì	Sì	No	No	No
AWS::IoTSiteWise:: AssetModel	No	No	Sì	Sì	No	No	No	No
AWS::IoTS iteWise::Dashboard	No	No	Sì	Sì	No	No	No	No
AWS::IoTS iteWise::Gateway	No	No	Sì	Sì	No	No	No	No
AWS::IoTSiteWise::Portal	No	No	Sì	Sì	No	No	No	No
AWS::IoTSiteWise::Project	No	No	Sì	Sì	No	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::IoTTwinMaker::ComponentType	No	No	Sì	Sì	No	No	No	No
AWS::IoTTwinMaker::Entity	No	No	Sì	Sì	No	No	No	No
AWS::IoTTwinMaker::Scene	No	No	Sì	Sì	No	No	No	No
AWS::IoTTwinMaker::SyncJob	No	No	Sì	Sì	No	No	No	No
AWS::IoTTwinMaker::Workspace	No	No	Sì	Sì	No	No	No	No
AWS::IoTWireless::FuotaTask	No	No	Sì	Sì	No	No	No	No
AWS::IoTWireless::MulticastGroup	No	No	Sì	Sì	No	No	No	No
AWS::IoTWireless::ServiceProfile	No	No	Sì	Sì	No	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::KMS::Alias	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::KMS::Key	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::KafkaConnect::Connector	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::Kendra::Index	No	No	Sì	No	Sì	No	No	No
AWS::Kinesis::Stream	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Kinesis::StreamConsumer	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::KinesisAnalyticsV2::Application	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::KinesisFirehose::DeliveryStream	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::KinesisVideo::SignalingChannel	No	Sì	Sì	Sì	Sì	No	No	No
AWS::KinesisVideo::Stream	No	Sì	Sì	Sì	Sì	No	No	No
AWS::Lambda::CodeSigningConfig	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Lambda::Function	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Lex::Bot	No	No	Sì	Sì	Sì	No	No	No
AWS::Lex::BotAlias	No	No	Sì	Sì	Sì	No	No	No
AWS::Lightsail::Bucket	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::Lightsail::Certificate	Sì	Sì	Sì	Sì	Sì	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Lightsail::Disk	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::Lightsail::StaticIp	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::Logs::Destination	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::LookoutMetrics::Alert	Sì	No	Sì	Sì	No	No	No	No
AWS::LookoutVision::Project	No	No	Sì	Sì	No	No	No	No
AWS::M2::Environment	No	Sì	Sì	Sì	Sì	No	No	No
AWS::MSK::BatchScramSegreto	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::MSK::Cluster	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::MSK::ClusterPolicy	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::MSK::Configuration	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::MSK::VpcConnection	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::MediaConnect::FlowEntitlement	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::MediaConnect::FlowSource	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::MediaConnect::FlowVpcInterfaccia	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::MediaPackage::PackagingConfiguration	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::MediaPackage::PackagingGroup	Sì	Sì	Sì	Sì	Sì	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::MediaTailor:: PlaybackConfiguration	No	No	Sì	Sì	No	No	No	No
AWS::Memo ryDB::SubnetGroup	Sì	No	Sì	Sì	Sì	No	No	No
AWS::Netw orkFirewall::Firewall	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::NetworkFirewa ll::FirewallPolicy	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::NetworkFirewa ll::RuleGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::NetworkFirewa ll: :TLS Inspectio nConfiguration	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Open Search::Domain	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Panorama::Package	No	No	Sì	No	No	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Personalize::Dataset	No	No	Sì	Sì	No	No	No	No
AWS::Personalize::DatasetGroup	No	No	Sì	Sì	No	No	No	No
AWS::Personalize::Schema	No	No	Sì	Sì	No	No	No	No
AWS::Personalize::Solution	No	No	Sì	Sì	No	No	No	No
AWS::Pinpoint::App	No	No	Sì	Sì	Sì	No	No	No
AWS::Pinpoint::ApplicationSettings	No	No	Sì	Sì	Sì	No	No	No
AWS::Pinpoint::Campaign	No	No	Sì	Sì	Sì	No	No	No
AWS::Pinpoint::EmailChannel	No	No	Sì	Sì	Sì	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Pinpoint::EmailTemplate	No	No	Sì	Sì	Sì	No	No	No
AWS::Pinpoint::EventStream	No	No	Sì	Sì	Sì	No	No	No
AWS::Pinpoint::InAppModello	No	No	Sì	Sì	Sì	No	No	No
AWS::Pinpoint::Segment	No	No	Sì	Sì	Sì	No	No	No
AWS::QLDB::Ledger	No	No	Sì	Sì	Sì	No	No	No
AWS::QuickSight::DataSource	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::QuickSight::Template	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::QuickSight::Theme	Sì	Sì	Sì	Sì	Sì	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::RDS::DBCluster	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì
AWS: :RDS: :DB ClusterSnapshot	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RDS::DBInstance	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS: :RDS: :DB SecurityGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RDS::DBSnapshot	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS: :RDS: :DB SubnetGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RDS: :EventSubscription	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RDS::GlobalCluster	No	Sì	Sì	Sì	Sì	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::RDS::OptionGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RUM::AppMonitor	Sì	No	Sì	Sì	Sì	No	No	No
AWS::Redshift::Cluster	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::Clu sterParameterGruppo	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::Clu sterSecurityGruppo	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::Clu sterSnapshot	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::Clu sterSubnetGruppo	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::End pointAccess	Sì	Sì	Sì	Sì	Sì	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Redshift::EndpointAuthorization	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::Redshift::EventSubscription	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::ScheduledAction	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::ResilienceHub::App	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::ResilienceHub::ResiliencyPolicy	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::ResourceExplorer2::Index	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::RoboMaker::RobotApplication	No	No	Sì	Sì	No	No	No	No
AWS::RoboMaker::RobotApplicationVersione	No	No	Sì	Sì	No	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::RoboMaker::Si mulationApplication	No	No	Sì	Sì	No	No	No	No
AWS::Route53Resolv er::FirewallDomainElenco	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Route53Resolv er::FirewallRuleGruppo	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Route53Resolv er::FirewallRuleGr oupAssociation	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Route53Resolv er::ResolverEndpoint	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Route53Resolv er::ResolverQueryL oggingConfig	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Route53Resolv er::ResolverQueryL oggingConfigAssociazione	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Route53Resolv er::ResolverRule	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Rout e53Resolver::Resol verRuleAssociazione	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::S3::AccessPoint	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::S3::AccountPu blicAccessBlock	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::S3::Bucket	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::S3::StorageLens	Sì	Sì	Sì	Sì	Sì	No	No	No
AWS::SES: :ConfigurationSet	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SES::ContactList	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SES::ReceiptFilter	No	No	Sì	No	No	No	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::SES::ReceiptRuleImpostare	No	No	Sì	No	No	No	No	No
AWS::SES::Template	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SNS::Topic	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SQS::Queue	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SSM::AssociationCompliance	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::SSM::Document	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::SSM::FileData	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::SSM::ManagedInstanceInventario	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::SSM::PatchCompliance	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::SageMaker::AppImageConfig	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SageMaker::CodeRepository	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SageMaker::Domain	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SageMaker::EndpointConfig	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SageMaker::FeatureGroup	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SageMaker::Image	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SageMaker::Model	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::SageMaker::NotebookInstance	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::SageMaker::Workteam	No	No	Sì	Sì	Sì	No	No	No
AWS::SecretsManager::Secret	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ServiceCatalog::CloudFormationProdotto	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ServiceCatalog::Portfolio	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ServiceDiscovery::HttpNamespace	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francoforte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolma)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::ServiceDiscovery::Instance	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::ServiceDiscovery::PublicDnsNamespace	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::ServiceDiscovery::Service	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::ShieldRegional::Protection	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Signer::SigningProfile	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::StepFunctions::Activity	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::StepFunctions::StateMachine	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Transfer::Agreement	Sì	Sì	Sì	Sì	Sì	Sì	No	No

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::Transfer::Certificate	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Transfer::Connector	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::Transfer::Profile	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Transfer::Workflow	Sì	Sì	Sì	Sì	Sì	Sì	No	No
AWS::WAFRegional:: RateBasedRegola	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFRegional::Rule	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFR egional::RuleGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFR egional::WebACL	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Europa (Irlanda)	Europa (Francofc rte)	Europa (Londra)	Europa (Parigi)	Europa (Stoccolm a)	Europa (Milano)	Europa (Spagna)	Europa (Zurigo)
AWS::WAFv2::IPSet	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFv2::Manage dRuleImpostare	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFv2::RegexP atternImpostare	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFv2::RuleGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFv2::WebACL	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WorkSpaces::C onnectionAlias	No	No	Sì	Sì	Sì	No	No	No
AWS::Work Spaces::Workspace	No	No	Sì	Sì	Sì	No	No	No
AWS::XRay ::EncryptionConfig	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Regioni dell'Asia Pacifico

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::ACM::Certificate	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ACMPCA::CertificateAuthority	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ACMPCA::CertificateAuthorityAttivazione	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::APS::RuleGroupsNamespace	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::AccessAnalyzer::Analyzer	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AmazonMQ::Broker	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Amplify::App	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::Amplify::Branch	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::ApiGateway::RestApi	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ApiGateway::Stage	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ApiGatewayV2::Api	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ApiGatewayV2::Stage	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AppConfig::Application	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AppConfig::ConfigurationProfile	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AppConfig::DeploymentStrategy	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AppConfig::Environment	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giakarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::AppConfig::ExtensionAssociation	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AppConfig::HostedConfigurationVersione	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AppFlow::Flow	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::AppIntegrations::EventIntegration	No	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::AppMesh::GatewayRoute	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::AppMesh::Mesh	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::AppMesh::Route	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::AppMesh::VirtualGateway	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::AppMesh::VirtualNode	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::AppMesh::VirtualRouter	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::AppMesh::VirtualService	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::AppRunner::Service	No	No	No	No	No	No	No	Sì	Sì	Sì
AWS::AppRunner::VpcConnector	No	No	No	No	No	No	No	Sì	No	No
AWS::AppStream::Application	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::AppStream::DirectoryConfig	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::AppStream::Fleet	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::AppStream::Stack	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::AppSync::GraphAPI QL	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì
AWS::Athena::DataCatalog	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Athena::PreparedStatement	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Athena::WorkGroup	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::AuditManager::Assessment	Sì	No	No	No	No	No	No	Sì	Sì	Sì
AWS::AutoScaling::AutoScalingGruppo	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AutoScaling::LaunchConfiguration	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::AutoScaling::ScalingPolicy	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AutoScaling::ScheduledAction	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::AutoScaling::WarmPool	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Backup::BackupPlan	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Backup::BackupSelection	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Backup::BackupVault	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Backup::RecoveryPoint	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Backup::ReportPlan	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::Batch::ComputeEnvironment	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì
AWS::Batch::JobQueue	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì
AWS::Batch::SchedulingPolicy	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì
AWS::Cassandra::Keyspace	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::Cloud9::EnvironmentEC2	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::CloudFormation::Stack	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::CloudTrail::Trail	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::CloudWatch::Alarm	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::CloudWatch::MetricStream	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::CodeArtifact::Repository	Sì	No	No	No	No	No	No	Sì	Sì	Sì
AWS::CodeBuild::Project	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::CodeBuild::ReportGroup	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::CodeDeploy::Application	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::CodeDeploy::DeploymentConfig	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::CodeDeploy::DeploymentGroup	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::CodeGuruProfiler::ProfilingGroup	No	No	No	No	No	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::CodeGuruReviewer::RepositoryAssociation	No	No	No	No	No	No	No	Sì	Sì	Sì
AWS::CodePipeline::Pipeline	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::Cognito::UserPool	Sì	No	No	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Cognito::UserPoolCliente	Sì	No	No	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Cognito::UserPoolGruppo	Sì	No	No	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Config::ConfigurationRecorder	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Config::ConformancePackConformità	Sì	No	Sì	No	Sì	No	Sì	Sì	Sì	Sì
AWS::Config::ResourceCompliance	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::Connect::Instance	No	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Connect::PhoneNumber	No	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Connect::QuickConnect	No	No	No	No	No	No	No	Sì	Sì	Sì
AWS::CustomerProfiles::Domain	No	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::CustomerProfiles::ObjectType	No	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::DMS::Certificate	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::DMS::Endpoint	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::DMS::EventSubscription	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::DMS::ReplicationInstance	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::DMS::ReplicationSubnetGruppo	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::DMS::ReplicationTask	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::DataSync::LocationEFS	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::DataSync::LocationF SxLustre	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::DataSync::LocationF SxWindows	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::DataSync::LocationHDFS	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::DataSync::LocationNFS	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::DataSync::LocationObjectArchiviazione	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì
AWS::DataSync::LocationS3	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì
AWS::DataSync::LocationSMB	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì
AWS::DataSync::Task	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Detective::Graph	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::DynamoDB::Table	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::Capacity Reservation	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::EC2::CarrierGateway	No	No	No	No	Sì	No	No	Sì	No	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::EC2::ClientVpnPunto finale	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::EC2::CustomerGateway	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::DHCPOptions	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì
AWS::EC2::EC2Fleet	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::EIP	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::EgressOnlyInternetGateway	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::EC2::FlowLog	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::EC2::Host	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::EC2::IPAM	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::IPAMPool	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::IPAMScope	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::Instance	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::InternetGateway	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::LaunchTemplate	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::EC2::NatGateway	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::EC2::NetworkAcl	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::EC2::NetworkInsightsAccessScope	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::EC2::NetworkInsightsAccessScopeAnalisi	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::EC2::NetworkInsightsAnalisi	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::EC2::NetworkInsightsPercorso	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::EC2::NetworkInterface	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::PrefixList	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::RegisteredIstanza Hain	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::EC2::RouteTable	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::EC2::SecurityGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::SpotFleet	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::Subnet	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::SubnetRouteTableAssociation	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::TrafficMirrorFiltro	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::EC2::TrafficMirrorSessione	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::EC2::TrafficMirrorObiettivo	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::EC2::TransitGateway	Sì	Sì	Sì	Sì	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::EC2::TransitGatewayAllegato	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì
AWS::EC2::TransitGatewayConnect	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::EC2::TransitGatewayMulticastDomain	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::TransitGatewayRouteTable	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::EC2::VPC	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::VPCEndpoint	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS: :EC2: :VPCEndpointService	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS: :EC2: :VPCPeeringConnection	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::EC2::VPNConnection	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::VPNGateway	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EC2::Volume	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECR::PullThroughCacheRule	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECR::RegistryPolicy	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECR::Repository	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECS::CapacityProvider	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECS::Cluster	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::ECS::Service	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECS::TaskDefinition	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ECS::TaskSet	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EFS::AccessPoint	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EFS::FileSystem	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EKS::Addon	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EKS::Cluster	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EKS::FargateProfile	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::EKS::IdentityProviderConfig	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EMR::SecurityConfiguration	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ElasticBeanstalk::Application	Sì	Sì	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::ElasticBeanstalk::ApplicationVersion	Sì	Sì	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::ElasticBeanstalk::Environment	Sì	Sì	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::ElasticLoadBalancing::LoadBalancer	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ElasticLoadBalancingV2::Listener	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::ElasticLoadBalancingV2::LoadBalancer	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::Elasticsearch::Domain	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::EventSchemas::Discoverer	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::EventSchemas::Registry	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::EventSchemas::RegistryPolicy	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::EventSchemas::Schema	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::Events::ApiDestination	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::Events::Archive	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì
AWS::Events::Connection	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::Events::Endpoint	Sì	No	No	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Events::EventBus	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Events::Rule	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Evidently::Launch	No	No	No	No	No	No	No	Sì	Sì	Sì
AWS::Evidently::Project	No	No	No	No	No	No	No	Sì	Sì	Sì
AWS::Evidently::Segment	No	No	No	No	No	No	No	Sì	Sì	Sì
AWS::FIS::ExperimentTemplate	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::Forecast::Dataset	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::Forecast::DatasetGroup	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::FraudDetector::EntityType	No	No	No	No	No	No	No	No	Sì	Sì
AWS::FraudDetector::Label	No	No	No	No	No	No	No	No	Sì	Sì
AWS::FraudDetector::Outcome	No	No	No	No	No	No	No	No	Sì	Sì
AWS::FraudDetector::Variable	No	No	No	No	No	No	No	No	Sì	Sì
AWS::Glue::Classifier	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Glue::Job	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Glue::MLTransform	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::Grafana::Workspace	No	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::GreengrassV2::ComponentVersion	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::GroundStation::Config	No	No	No	No	Sì	No	No	No	Sì	Sì
AWS::GroundStation::DataflowEndpointGruppo	No	No	No	No	Sì	No	No	No	Sì	Sì
AWS::GroundStation::MissionProfile	No	No	No	No	Sì	No	No	No	Sì	Sì
AWS::GuardDuty::Detector	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::GuardDuty::Filter	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::GuardDovere: :IPSet	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::GuardDuty::ThreatIntelImpostare	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::HealthLake::FHIRData Store	Sì	No	No	No	No	No	No	No	No	No
AWS::IAM::Group	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::IAM::Policy	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::IAM::Role	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::IAM::User	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::IVS::Channel	Sì	No	No	No	Sì	No	No	Sì	No	No
AWS::IVS::Playback KeyCoppia	Sì	No	No	No	Sì	No	No	Sì	No	No

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giakarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::IVS::RecordingConfiguration	Sì	No	No	No	Sì	No	No	No	No	No
AWS::ImageBuilder::ContainerRecipe	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ImageBuilder::DistributionConfiguration	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::ImageBuilder::ImagePipeline	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ImageBuilder::ImageRecipe	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::ImageBuilder::InfrastructureConfiguration	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::InspectorV2::Filter	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::IoT::AccountAuditConfigurazione	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::IoT::Authorizer	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::IoCertificato T: :CA	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::IoT::CustomMetric	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::IoT::Dimension	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::IoT::FleetMetric	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::IoT::JobTemplate	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::IoT::MitigationAction	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::IoT::Policy	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::IoT::ProvisioningTemplate	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::IoT::RoleAlias	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::IoT::ScheduledAudit	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::IoT::SecurityProfile	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::IoTAnalytics::Channel	Sì	No	No	No	No	No	No	Sì	No	Sì
AWS::IoTAnalytics::Dataset	Sì	No	No	No	No	No	No	Sì	No	Sì
AWS::IoTAnalytics::Datastore	Sì	No	No	No	No	No	No	Sì	No	Sì
AWS::IoTAnalytics::Pipeline	Sì	No	No	No	No	No	No	Sì	No	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::IoTEvents::AlarmModel	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::IoTEvents::DetectorModel	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::IoTEvents::Input	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::IoTSiteWise::AssetModel	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::IoTSiteWise::Dashboard	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::IoTSiteWise::Gateway	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::IoTSiteWise::Portal	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::IoTSiteWise::Project	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::IoTTwinMaker::ComponentType	No	No	No	No	No	No	No	No	Sì	Sì
AWS::IoTTwinMaker::Entity	No	No	No	No	No	No	No	No	Sì	Sì
AWS::IoTTwinMaker::Scene	No	No	No	No	No	No	No	No	Sì	Sì
AWS::IoTTwinMaker::SyncJob	No	No	No	No	No	No	No	No	Sì	Sì
AWS::IoTTwinMaker::Workspace	No	No	No	No	No	No	No	No	Sì	Sì
AWS::IoTWireless::FuotaTask	No	No	No	No	No	No	No	Sì	No	Sì
AWS::IoTWireless::MulticastGroup	No	No	No	No	No	No	No	Sì	No	Sì
AWS::IoTWireless::ServiceProfile	No	No	No	No	No	No	No	Sì	No	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::KMS::Alias	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::KMS::Key	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::KafkaConnect::Connector	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Kendra::Index	Sì	No	No	No	No	No	No	Sì	Sì	Sì
AWS::Kinesis::Stream	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Kinesis::StreamConsumer	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::KinesisAnalyticsV2::Application	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::KinesisFirehose::DeliveryStream	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::KinesisVideo::SignalingChannel	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::KinesisVideo::Stream	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::Lambda::CodeSigningConfig	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::Lambda::Function	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Lex::Bot	No	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Lex::BotAlias	No	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Lightsail::Bucket	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Lightsail::Certificate	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::Lightsail::Disk	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Lightsail::StaticIp	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Logs::Destination	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::LookoutMetrics::Alert	No	No	No	No	No	No	No	Sì	Sì	Sì
AWS::LookoutVision::Project	No	No	No	No	Sì	No	No	Sì	No	No
AWS::M2::Environment	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::MSK::BatchScramSegreto	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::MSK::Cluster	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::MSK::ClusterPolicy	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::MSK::Configuration	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::MSK::VpcConnection	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::MediaConnect::FlowEntitlement	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::MediaConnect::FlowSource	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::MediaConnect::FlowVpcInterfaccia	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::MediaPackage::PackagingConfiguration	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::MediaPackage::PackagingGroup	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::MediaTailor::PlaybackConfiguration	Sì	No	No	No	No	No	No	Sì	Sì	Sì
AWS::MemoryDB::SubnetGroup	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::NetworkFirewall::Firewall	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::NetworkFirewall::FirewallPolicy	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::NetworkFirewall::RuleGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::NetworkFirewall: :TLS InspectionConfiguration	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::OpenSearch::Domain	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Panorama::Package	No	No	No	No	No	No	No	No	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::Personalize::Dataset	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Personalize::DatasetGroup	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Personalize::Schema	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Personalize::Solution	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Pinpoint::App	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Pinpoint::ApplicationSettings	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Pinpoint::Campaign	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Pinpoint::EmailChannel	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::Pinpoint::EmailTemplate	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Pinpoint::EventStream	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Pinpoint::InAppModello	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Pinpoint::Segment	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::QLDB::Ledger	No	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::QuickSight::DataSource	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::QuickSight::Template	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::QuickSight::Theme	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::RDS::DBCluster	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS: :RDS: :DB ClusterSnapshot	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RDS: :DBInstance	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS: :RDS: :DB SecurityGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RDS: :DBSnapshot	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS: :RDS: :DB SubnetGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RDS: :EventSubscription	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RDS: :GlobalCluster	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::RDS::OptionGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::RUM::AppMonitor	No	No	No	No	No	No	No	Sì	Sì	Sì
AWS::Redshift::Cluster	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::ClusterParameterGruppo	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::ClusterSecurityGruppo	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::ClusterSnapshot	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::ClusterSubnetGruppo	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::EndpointAccess	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::Redshift::EndpointAuthorization	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::Redshift::EventSubscription	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Redshift::ScheduledAction	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::ResilienceHub::App	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::ResilienceHub::ResiliencyPolicy	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::ResourceExplorer2::Index	Sì	No	No	No	Sì	Sì	No	Sì	Sì	Sì
AWS::RoboMaker::RobotApplication	No	No	No	No	No	No	No	Sì	Sì	No
AWS::RoboMaker::RobotApplicationVersione	No	No	No	No	No	No	No	Sì	Sì	No

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::RoboMaker::SimulationApplication	No	No	No	No	No	No	No	Sì	Sì	No
AWS::Route53Resolver::FirewallDomainElenco	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Route53Resolver::FirewallRuleGruppo	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Route53Resolver::ResolverEndpoint	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociazione	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Route53Resolver::ResolverRule	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::Route53Resolver::ResolverRuleAssociazione	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::S3::AccessPoint	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::S3::AccountPublicAccessBlock	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::S3::Bucket	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::S3::StorageLens	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::SES::ConfigurationSet	Sì	Sì	No	No	Sì	Sì	No	Sì	Sì	Sì
AWS::SES::ContactList	Sì	Sì	No	No	Sì	Sì	No	Sì	Sì	Sì
AWS::SES::Template	Sì	Sì	No	No	Sì	Sì	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::SNS::Topic	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::SQS::Queue	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::SSM::AssociationCompliance	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì
AWS::SSM::Document	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::SSM::FileData	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì
AWS::SSM::ManagedInstanceInventario	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::SSM::PatchCompliance	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì
AWS::SageMaker::AppImageConfig	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::SageMaker::CodeRepository	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::SageMaker::Domain	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::SageMaker::EndpointConfig	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::SageMaker::FeatureGroup	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::SageMaker::Image	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::SageMaker::Model	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::SageMaker::NotebookInstance	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sì	No	Sì	No	Sì	Sì	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::SageMaker::Workteam	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::SecretsManager::Secret	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ServiceCatalog::CloudFormationProdotto	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ServiceCatalog::Portfolio	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::ServiceDiscovery::HttpNamespace	Sì	No	Sì	No	Sì	No	Sì	Sì	Sì	Sì
AWS::ServiceDiscovery::Instance	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::ServiceDiscovery::PublicDnsNamespace	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::ServiceDiscovery::Service	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::ShieldRegional::Protection	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Signer::SigningProfile	Sì	No	Sì	No	Sì	No	No	Sì	Sì	Sì
AWS::StepFunctions::Activity	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì
AWS::StepFunctions::StateMachine	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì	Sì	Sì
AWS::Transfer::Agreement	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Transfer::Certificate	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::Transfer::Connector	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::Transfer::Profile	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::Transfer::Workflow	Sì	Sì	Sì	No	Sì	Sì	No	Sì	Sì	Sì
AWS::WAFRegional::RateBasedRegola	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFRegional::Rule	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFRegional::RuleGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFRegional::WebACL	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFv2::IPSet	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFv2::ManagedRuleImpostare	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Tipo di risorsa	Asia Pacifico (Singapore)	Asia Pacifico (Tokyo)	Asia Pacifico (Sydney)	Asia Pacifico (Seoul)	Asia Pacifico (Mumbai)	Asia Pacifico (Osaka-Locale)	Asia Pacifico (Hong Kong)	Asia Pacifico (Giacarta)	Asia Pacifico (Hyderabad)	Asia Pacifico (Melbourne)
AWS::WAFv2::RegexPatternImpostare	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFv2::RuleGroup	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WAFv2::WebACL	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AWS::WorkSpaces::ConnectionAlias	No	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::WorkSpaces::Workspace	Sì	No	No	No	Sì	No	No	Sì	Sì	Sì
AWS::XRay::EncryptionConfig	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì

Regioni della Cina

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::ACM::Certificate	Sì	Sì
AWS::AmazonMQ::Broker	Sì	Sì
AWS::ApiGateway::RestApi	Sì	Sì
AWS::ApiGateway::Stage	Sì	Sì
AWS::ApiGatewayV2::Api	Sì	Sì
AWS::ApiGatewayV2::Stage	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::AppConfig::Application	Sì	Sì
AWS::AppConfig::ConfigurationProfile	Sì	Sì
AWS::AppConfig::DeploymentStrategy	Sì	Sì
AWS::AppConfig::Environment	Sì	Sì
AWS::AppConfig::ExtensionAssociation	Sì	Sì
AWS::AppConfig::HostedConfigurationversione	Sì	Sì
AWS::AppSync::GraphQLAPI	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::Athena::DataCatalog	Sì	Sì
AWS::Athena::PreparedStatement	Sì	Sì
AWS::Athena::WorkGroup	Sì	Sì
AWS::AutoScaling::AutoScalingGruppo	Sì	Sì
AWS::AutoScaling::LaunchConfiguration	Sì	Sì
AWS::AutoScaling::ScalingPolicy	Sì	Sì
AWS::AutoScaling::ScheduledAction	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::AutoScaling::WarmPool	Sì	Sì
AWS::Backup::BackupPlan	Sì	Sì
AWS::Backup::BackupSelection	Sì	Sì
AWS::Backup::BackupVault	Sì	Sì
AWS::Backup::RecoveryPoint	Sì	Sì
AWS::Batch::ComputeEnvironment	Sì	Sì
AWS::Batch::JobQueue	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::Batch::SchedulingPolicy	Sì	Sì
AWS::Cassandra::Keyspace	Sì	Sì
AWS::CloudFormation::Stack	Sì	Sì
AWS::CloudTrail::Trail	Sì	Sì
AWS::CloudWatch::Alarm	Sì	Sì
AWS::CloudWatch::MetricStream	Sì	Sì
AWS::CodeBuild::Project	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::CodeBuild::ReportGroup	Sì	Sì
AWS::Config::ConfigurationRecorder	Sì	Sì
AWS::Config::ResourceCompliance	Sì	Sì
AWS::DMS::Certificate	Sì	Sì
AWS::DMS::Endpoint	Sì	Sì
AWS::DMS::EventSubscription	Sì	Sì
AWS::DMS::ReplicationInstance	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::DMS::ReplicationSubnetGruppo	Sì	Sì
AWS::DMS::ReplicationTask	Sì	Sì
AWS::DataSync::LocationEFS	Sì	Sì
AWS::DataSync::LocationHDFS	Sì	Sì
AWS::DataSync::LocationNFS	Sì	Sì
AWS::DataSync::LocationObjectArchiviazione	Sì	Sì
AWS::DataSync::LocationS3	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::DataSync::LocationSMB	Sì	Sì
AWS::DataSync::Task	Sì	Sì
AWS::DynamoDB::Table	Sì	Sì
AWS::EC2::CapacityReservation	Sì	Sì
AWS::EC2::DHCPOptions	Sì	Sì
AWS::EC2::EC2Fleet	Sì	Sì
AWS::EC2::EIP	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::EC2::FlowLog	Sì	Sì
AWS::EC2::Host	Sì	Sì
AWS::EC2::Instance	Sì	Sì
AWS::EC2::InternetGateway	Sì	Sì
AWS::EC2::LaunchTemplate	Sì	Sì
AWS::EC2::NatGateway	Sì	Sì
AWS::EC2::NetworkAcl	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::EC2::NetworkInterface	Sì	Sì
AWS::EC2::PrefixList	Sì	Sì
AWS::EC2::RouteTable	Sì	Sì
AWS::EC2::SecurityGroup	Sì	Sì
AWS::EC2::SpotFleet	Sì	Sì
AWS::EC2::Subnet	Sì	Sì
AWS::EC2::SubnetRouteTableAssociation	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::EC2::TrafficMirrorFiltro	Sì	Sì
AWS::EC2::TrafficMirrorSessione	Sì	Sì
AWS::EC2::TrafficMirrorObiettivo	Sì	Sì
AWS::EC2::TransitGateway	Sì	Sì
AWS::EC2::TransitGatewayAllegato	Sì	Sì
AWS::EC2::TransitGatewayConnect	Sì	Sì
AWS::EC2::TransitGatewayMulticastDomain	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::EC2::TransitGatewayRouteTable	Sì	Sì
AWS::EC2::VPC	Sì	Sì
AWS::EC2::VPCEndpoint	Sì	Sì
AWS: :EC2: :VPC EndpointService	Sì	Sì
AWS: :EC2: :VPC PeeringConnection	Sì	Sì
AWS::EC2::VPNGateway	Sì	No
AWS::EC2::Volume	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::ECR::Repository	Sì	Sì
AWS::ECS::CapacityProvider	Sì	Sì
AWS::ECS::Cluster	Sì	Sì
AWS::ECS::Service	Sì	Sì
AWS::ECS::TaskDefinition	Sì	Sì
AWS::ECS::TaskSet	Sì	Sì
AWS::EFS::AccessPoint	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::EFS::FileSystem	Sì	Sì
AWS::EKS::Addon	Sì	Sì
AWS::EKS::Cluster	Sì	Sì
AWS::EKS::FargateProfile	Sì	Sì
AWS::EKS::IdentityProviderConfig	Sì	Sì
AWS::EMR::SecurityConfiguration	Sì	Sì
AWS::ElasticBeanstalk::Application	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::ElasticBeanstalk::ApplicationVersion	Sì	Sì
AWS::ElasticBeanstalk::Environment	Sì	Sì
AWS::ElasticLoadBalancing::LoadBalancer	Sì	Sì
AWS::ElasticLoadBalancingV2::Listener	Sì	Sì
AWS::ElasticLoadBalancingV2::LoadBalancer	Sì	Sì
AWS::Elasticsearch::Domain	Sì	Sì
AWS::Events::Archive	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::Events::EventBus	Sì	Sì
AWS::Events::Rule	Sì	Sì
AWS::Glue::Classifier	Sì	Sì
AWS::Glue::Job	Sì	Sì
AWS::Glue:: MLTransform	Sì	No
AWS::GreengrassV2::ComponentVersion	Sì	No
AWS::GuardDuty::Filter	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::GuardDuty::ThreatIntelImpostare	Sì	Sì
AWS::IAM::Group	Sì	Sì
AWS::IAM::InstanceProfile	Sì	No
AWS::IAM::OIDCProvider	Sì	No
AWS::IAM::Policy	Sì	Sì
AWS::IAM::Role	Sì	Sì
AWS::IAM::SAMLProvider	Sì	No

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::IAM::ServerCertificate	Sì	No
AWS::IAM::User	Sì	Sì
AWS::ImageBuilder::ContainerRecipe	Sì	Sì
AWS::ImageBuilder::DistributionConfiguration	Sì	Sì
AWS::ImageBuilder::ImagePipeline	Sì	Sì
AWS::ImageBuilder::ImageRecipe	Sì	Sì
AWS::ImageBuilder::InfrastructureConfiguration	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::IoT::AccountAuditConfigurazione	Sì	Sì
AWS::IoT::Authorizer	Sì	Sì
AWS::IoCertificato T: :CA	Sì	Sì
AWS::IoT::CustomMetric	Sì	Sì
AWS::IoT::Dimension	Sì	Sì
AWS::IoT::FleetMetric	Sì	Sì
AWS::IoT::JobTemplate	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::IoT::MitigationAction	Sì	Sì
AWS::IoT::Policy	Sì	Sì
AWS::IoT::ProvisioningTemplate	Sì	Sì
AWS::IoT::RoleAlias	Sì	Sì
AWS::IoT::ScheduledAudit	Sì	Sì
AWS::IoT::SecurityProfile	Sì	Sì
AWS::IoTAnalytics::Channel	Sì	No

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::IoTAnalytics::Dataset	Sì	No
AWS::IoTAnalytics::Datastore	Sì	No
AWS::IoTAnalytics::Pipeline	Sì	No
AWS::IoTEvents::AlarmModel	Sì	No
AWS::IoTEvents::DetectorModel	Sì	No
AWS::IoTEvents::Input	Sì	No
AWS::IoTSiteWise::AssetModel	Sì	No

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::IoTSiteWise::Dashboard	Sì	No
AWS::IoTSiteWise::Gateway	Sì	No
AWS::IoTSiteWise::Portal	Sì	No
AWS::IoTSiteWise::Project	Sì	No
AWS::KMS::Alias	Sì	Sì
AWS::KMS::Key	Sì	Sì
AWS::Kinesis::Stream	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::Kinesis::StreamConsumer	Sì	Sì
AWS::KinesisAnalyticsV2::Application	Sì	Sì
AWS::KinesisFirehose::DeliveryStream	Sì	Sì
AWS::Lambda::Function	Sì	No
AWS::Logs::Destination	Sì	Sì
AWS::MSK::BatchScramSegreto	Sì	Sì
AWS::MSK::Cluster	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::MSK::ClusterPolicy	Sì	Sì
AWS::MSK::Configuration	Sì	Sì
AWS::MSK::VpcConnection	Sì	Sì
AWS::NetworkFirewall::Firewall	Sì	Sì
AWS::NetworkFirewall::FirewallPolicy	Sì	Sì
AWS::NetworkFirewall::RuleGroup	Sì	Sì
AWS::NetworkFirewall: :TLS InspectionConfiguration	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::OpenSearch::Domain	Sì	Sì
AWS::Personalize::Dataset	Sì	No
AWS::Personalize::DatasetGroup	Sì	No
AWS::Personalize::Schema	Sì	No
AWS::Personalize::Solution	Sì	No
AWS::RDS::DBCluster	No	Sì
AWS: :RDS: :DB ClusterSnapshot	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::RDS::DBInstance	Sì	Sì
AWS: :RDS: :DB SecurityGroup	Sì	Sì
AWS::RDS::DBSnapshot	Sì	Sì
AWS: :RDS: :DB SubnetGroup	Sì	Sì
AWS::RDS::EventSubscription	Sì	Sì
AWS::RDS::OptionGroup	Sì	Sì
AWS::Redshift::Cluster	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::Redshift::ClusterParameterGruppo	Sì	Sì
AWS::Redshift::ClusterSecurityGruppo	Sì	Sì
AWS::Redshift::ClusterSnapshot	Sì	Sì
AWS::Redshift::ClusterSubnetGruppo	Sì	Sì
AWS::Redshift::EventSubscription	Sì	Sì
AWS::Route53Resolver::FirewallDomainElenco	Sì	Sì
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::Route53Resolver::ResolverEndpoint	Sì	Sì
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sì	Sì
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociazione	Sì	Sì
AWS::Route53Resolver::ResolverRule	Sì	Sì
AWS::Route53Resolver::ResolverRuleAssociazione	Sì	Sì
AWS::S3::AccessPoint	Sì	Sì
AWS::S3::AccountPublicAccessBlock	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::S3::Bucket	Sì	Sì
AWS::SES::ConfigurationSet	No	Sì
AWS::SES::ContactList	No	Sì
AWS::SES::Template	No	Sì
AWS::SNS::Topic	Sì	Sì
AWS::SQS::Queue	Sì	Sì
AWS::SSM::AssociationCompliance	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::SSM::Document	Sì	Sì
AWS::SSM::FileData	Sì	Sì
AWS::SSM::ManagedInstanceInventario	Sì	Sì
AWS::SSM::PatchCompliance	Sì	Sì
AWS::SageMaker::AppImageConfig	Sì	Sì
AWS::SageMaker::CodeRepository	Sì	Sì
AWS::SageMaker::Domain	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::SageMaker::EndpointConfig	Sì	Sì
AWS::SageMaker::FeatureGroup	Sì	Sì
AWS::SageMaker::Image	Sì	Sì
AWS::SageMaker::Model	Sì	Sì
AWS::SageMaker::NotebookInstance	Sì	Sì
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sì	Sì
AWS::SecretsManager::Secret	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::ServiceCatalog::CloudFormationProdotto	Sì	Sì
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sì	Sì
AWS::ServiceCatalog::Portfolio	Sì	Sì
AWS::ServiceDiscovery::HttpNamespace	Sì	Sì
AWS::ServiceDiscovery::Instance	Sì	Sì
AWS::ServiceDiscovery::PublicDnsNamespace	Sì	Sì
AWS::ServiceDiscovery::Service	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::StepFunctions::Activity	Sì	No
AWS::StepFunctions::StateMachine	Sì	Sì
AWS::Transfer::Agreement	Sì	Sì
AWS::Transfer::Certificate	Sì	Sì
AWS::Transfer::Connector	Sì	Sì
AWS::Transfer::Profile	Sì	Sì
AWS::Transfer::Workflow	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::WAFRegional::RateBasedRegola	Sì	Sì
AWS::WAFRegional::Rule	Sì	Sì
AWS::WAFRegional::RuleGroup	Sì	Sì
AWS::WAFRegional::WebACL	Sì	Sì
AWS::WAFv2::IPSet	Sì	Sì
AWS::WAFv2::ManagedRuleImpostare	Sì	Sì
AWS::WAFv2::RegexPatternImpostare	Sì	Sì

Tipo di risorsa	Cina (Pechino)	Cina (Ningxia)
AWS::WAFv2::RuleGroup	Sì	Sì
AWS::WAFv2::WebACL	Sì	Sì
AWS::WorkSpaces::Workspace	No	Sì

Regioni dell'Africa e del Medio Oriente

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::ACM::Certificate	Sì	Sì	Sì	Sì
AWS::ACMPCA::CertificateAuthority	Sì	Sì	Sì	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::ACMPCA::CertificateAuthorityAttivazione	Sì	Sì	Sì	No
AWS::AccessAnalyzer::Analyzer	Sì	Sì	Sì	No
AWS::AmazonMQ::Broker	Sì	Sì	Sì	No
AWS::Amplify::App	Sì	No	No	No
AWS::Amplify::Branch	Sì	No	No	No
AWS::ApiGateway::RestApi	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::ApiGateway::Stage	Sì	Sì	Sì	Sì
AWS::ApiGatewayV2::Api	Sì	Sì	Sì	Sì
AWS::ApiGatewayV2::Stage	Sì	Sì	Sì	Sì
AWS::AppConfig::Application	Sì	Sì	No	Sì
AWS::AppConfig::ConfigurationProfile	Sì	Sì	No	Sì
AWS::AppConfig::DeploymentStrategy	Sì	Sì	No	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::AppConfig::Environment	Sì	Sì	No	Sì
AWS::AppConfig::ExtensionAssociation	Sì	Sì	Sì	Sì
AWS::AppConfig::HostedConfigurationVersione	Sì	Sì	No	Sì
AWS::AppIntegrations::EventIntegration	No	Sì	No	No
AWS::AppMesh::GatewayRoute	Sì	Sì	No	No
AWS::AppMesh::Mesh	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::AppMesh::Route	Sì	Sì	No	No
AWS::AppMesh::VirtualGateway	Sì	Sì	No	No
AWS::AppMesh::VirtualNode	Sì	Sì	No	No
AWS::AppMesh::VirtualRouter	Sì	Sì	No	No
AWS::AppMesh::VirtualService	Sì	Sì	No	No
AWS::AppSync::GraphQLAPI	Sì	Sì	Sì	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::Athena::DataCatalog	Sì	Sì	Sì	No
AWS::Athena::PreparedStatement	Sì	Sì	No	No
AWS::Athena::WorkGroup	Sì	Sì	Sì	No
AWS::AutoScaling::AutoScalingGruppo	Sì	Sì	Sì	Sì
AWS::AutoScaling::LaunchConfiguration	Sì	Sì	Sì	Sì
AWS::AutoScaling::ScalingPolicy	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::AutoScaling::ScheduledAction	Sì	Sì	Sì	Sì
AWS::AutoScaling::WarmPool	Sì	Sì	No	No
AWS::Backup::BackupPlan	Sì	Sì	No	No
AWS::Backup::BackupSelection	Sì	Sì	Sì	No
AWS::Backup::BackupVault	Sì	Sì	Sì	No
AWS::Backup::RecoveryPoint	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::Backup::ReportPlan	Sì	Sì	No	No
AWS::Batch::ComputeEnvironment	Sì	Sì	Sì	No
AWS::Batch::JobQueue	Sì	Sì	Sì	No
AWS::Batch::SchedulingPolicy	Sì	Sì	Sì	No
AWS::Cassandra::Keyspace	Sì	No	No	No
AWS::Cloud9::EnvironmentEC2	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::CloudFormation::Stack	Sì	Sì	No	No
AWS::CloudTrail::Trail	Sì	Sì	Sì	Sì
AWS::CloudWatch::Alarm	Sì	Sì	Sì	Sì
AWS::CloudWatch::MetricStream	Sì	Sì	Sì	Sì
AWS::CodeBuild::Project	Sì	Sì	Sì	Sì
AWS::CodeBuild::ReportGroup	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::CodeDeploy::Application	Sì	Sì	No	No
AWS::CodeDeploy::DeploymentConfig	Sì	Sì	No	No
AWS::CodeDeploy::DeploymentGroup	Sì	Sì	No	No
AWS::Cognito::UserPool	Sì	No	No	Sì
AWS::Cognito::UserPoolCliente	Sì	No	No	Sì
AWS::Cognito::UserPoolGruppo	Sì	No	No	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::Config::ConfigurationRecorder	Sì	Sì	Sì	Sì
AWS::Config::ConformancePackConformità	Sì	No	No	No
AWS::Config::ResourceCompliance	Sì	Sì	Sì	Sì
AWS::Connect::Instance	No	Sì	No	No
AWS::CustomerProfiles::Domain	No	Sì	No	No
AWS::CustomerProfiles::ObjectType	No	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::DMS::Certificate	Sì	Sì	No	No
AWS::DMS::Endpoint	Sì	Sì	No	No
AWS::DMS::EventSubscription	Sì	Sì	No	No
AWS::DMS::ReplicationInstance	Sì	Sì	No	No
AWS::DMS::ReplicationSubnetGruppo	Sì	Sì	No	No
AWS::DMS::ReplicationTask	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::DataSync::LocationEFS	Sì	Sì	Sì	No
AWS::DataSync::LocationF SxLustre	Sì	Sì	No	No
AWS::DataSync::LocationF SxWindows	Sì	Sì	No	No
AWS::DataSync::LocationHDFS	Sì	Sì	Sì	No
AWS::DataSync::LocationNFS	Sì	Sì	Sì	No
AWS::DataSync::Loc ationObjectArchiviazione	Sì	Sì	Sì	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::DataSync::LocationS3	Sì	Sì	Sì	No
AWS::DataSync::LocationSMB	Sì	Sì	Sì	No
AWS::DataSync::Task	Sì	Sì	Sì	No
AWS::Detective::Graph	Sì	Sì	No	No
AWS::DynamoDB::Table	Sì	Sì	Sì	Sì
AWS::EC2::CapacityReservation	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::EC2::ClientVpnPunto finale	Sì	Sì	No	No
AWS::EC2::CustomerGateway	Sì	Sì	Sì	Sì
AWS::EC2::DHCPOptions	Sì	Sì	Sì	Sì
AWS::EC2::EC2Fleet	Sì	Sì	Sì	No
AWS::EC2::EIP	Sì	Sì	Sì	Sì
AWS::EC2::EgressOnlyInternetGateway	Sì	Sì	Sì	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::EC2::FlowLog	Sì	Sì	Sì	No
AWS::EC2::Host	Sì	Sì	Sì	Sì
AWS::EC2::IPAM	Sì	Sì	Sì	No
AWS::EC2::IPAMPool	Sì	Sì	Sì	No
AWS::EC2::IPAMScope	Sì	Sì	Sì	No
AWS::EC2::Instance	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::EC2::InternetGateway	Sì	Sì	Sì	Sì
AWS::EC2::LaunchTemplate	Sì	Sì	No	No
AWS::EC2::NatGateway	Sì	Sì	Sì	No
AWS::EC2::NetworkAcl	Sì	Sì	Sì	Sì
AWS::EC2::NetworkInsightsAccessScope	Sì	Sì	No	No
AWS::EC2::NetworkInsightsAccessScopeAnalisi	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::EC2::NetworkInsightsAnalisi	Sì	Sì	No	No
AWS::EC2::NetworkInsightsPercorso	Sì	Sì	No	No
AWS::EC2::NetworkInterface	Sì	Sì	Sì	Sì
AWS::EC2::PrefixList	Sì	Sì	Sì	Sì
AWS::EC2::RouteTable	Sì	Sì	Sì	Sì
AWS::EC2::SecurityGroup	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::EC2::SpotFleet	Sì	Sì	Sì	Sì
AWS::EC2::Subnet	Sì	Sì	Sì	Sì
AWS::EC2::SubnetRouteTableAssociation	Sì	Sì	Sì	Sì
AWS::EC2::TrafficMirrorFiltro	Sì	No	No	No
AWS::EC2::TrafficMirrorSessione	Sì	No	No	No
AWS::EC2::TrafficMirrorObiettivo	Sì	No	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::EC2::TransitGateway	Sì	Sì	Sì	No
AWS::EC2::TransitGatewayAllegato	Sì	Sì	Sì	No
AWS::EC2::TransitGatewayConnect	Sì	Sì	Sì	No
AWS::EC2::TransitGatewayMulticastDomain	Sì	Sì	Sì	Sì
AWS::EC2::TransitGatewayRouteTable	Sì	Sì	Sì	No
AWS::EC2::VPC	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::EC2::VPCEndpoint	Sì	Sì	Sì	Sì
AWS: :EC2: :VPC EndpointService	Sì	Sì	Sì	Sì
AWS: :EC2: :VPC PeeringConnection	Sì	Sì	Sì	Sì
AWS::EC2::VPNConnection	Sì	Sì	Sì	Sì
AWS::EC2::VPNGateway	Sì	Sì	Sì	Sì
AWS::EC2::Volume	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::ECR::PullThroughCacheRule	Sì	Sì	Sì	Sì
AWS::ECR::RegistryPolicy	Sì	Sì	Sì	No
AWS::ECR::Repository	Sì	Sì	Sì	No
AWS::ECS::CapacityProvider	Sì	Sì	Sì	Sì
AWS::ECS::Cluster	Sì	Sì	Sì	Sì
AWS::ECS::Service	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::ECS::TaskDefinition	Sì	Sì	Sì	Sì
AWS::ECS::TaskSet	Sì	Sì	Sì	No
AWS::EFS::AccessPoint	Sì	Sì	Sì	No
AWS::EFS::FileSystem	Sì	Sì	Sì	No
AWS::EKS::Addon	Sì	Sì	Sì	No
AWS::EKS::Cluster	Sì	Sì	Sì	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::EKS::FargateProfile	Sì	Sì	Sì	Sì
AWS::EKS::IdentityProviderConfig	Sì	Sì	Sì	No
AWS::EMR::SecurityConfiguration	Sì	Sì	Sì	No
AWS::ElasticBeanstalk::Application	No	Sì	No	No
AWS::ElasticBeanstalk::ApplicationVersion	No	Sì	No	No
AWS::ElasticBeanstalk::Environment	No	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::ElasticLoadBalancing::LoadBalancer	Sì	Sì	Sì	Sì
AWS::ElasticLoadBalancingV2::Listener	Sì	Sì	No	No
AWS::ElasticLoadBalancingV2::LoadBalancer	Sì	Sì	Sì	Sì
AWS::Elasticsearch::Domain	Sì	Sì	Sì	Sì
AWS::Events::ApiDestination	Sì	Sì	No	No
AWS::Events::Archive	Sì	Sì	Sì	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::Events::Connection	Sì	Sì	No	No
AWS::Events::EventBus	Sì	Sì	No	No
AWS::Events::Rule	Sì	Sì	No	No
AWS::FIS::ExperimentTemplate	Sì	Sì	No	No
AWS::Glue::Classifier	Sì	Sì	Sì	Sì
AWS::Glue::Job	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::Glue:: MLTransform	Sì	Sì	Sì	Sì
AWS::GroundStation::Config	Sì	Sì	No	No
AWS::GroundStation ::DataflowEndpointGruppo	Sì	Sì	No	No
AWS::GroundStation::MissionProfile	Sì	Sì	No	No
AWS::GuardDuty::Detector	Sì	Sì	No	No
AWS::GuardDuty::Filter	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::GuardDovere: :IPSet	Sì	Sì	No	No
AWS::GuardDuty::ThreatIntelImpostare	Sì	Sì	No	No
AWS::IAM::Group	Sì	Sì	No	No
AWS::IAM::Policy	Sì	Sì	No	No
AWS::IAM::Role	Sì	Sì	No	No
AWS::IAM::User	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::ImageBuilder::ContainerRecipe	Sì	Sì	Sì	Sì
AWS::ImageBuilder::DistributionConfiguration	Sì	Sì	No	No
AWS::ImageBuilder::ImagePipeline	Sì	Sì	Sì	Sì
AWS::ImageBuilder::ImageRecipe	Sì	Sì	No	No
AWS::ImageBuilder::InfrastructureConfiguration	Sì	Sì	Sì	Sì
AWS::InspectorV2::Filter	Sì	No	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::IoT::AccountAuditConfigurazione	Sì	No	Sì	No
AWS::IoT::Authorizer	Sì	No	Sì	No
AWS::IoCertificato T: :CA	Sì	No	Sì	No
AWS::IoT::CustomMetric	Sì	No	Sì	No
AWS::IoT::Dimension	Sì	No	Sì	No
AWS::IoT::FleetMetric	Sì	No	Sì	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::IoT::JobTemplate	Sì	No	Sì	No
AWS::IoT::MitigationAction	Sì	No	Sì	No
AWS::IoT::Policy	Sì	No	Sì	No
AWS::IoT::ProvisioningTemplate	Sì	No	Sì	No
AWS::IoT::RoleAlias	Sì	No	Sì	No
AWS::IoT::ScheduledAudit	Sì	No	Sì	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::IoT::SecurityProfile	Sì	No	Sì	No
AWS::KMS::Alias	Sì	Sì	No	No
AWS::KMS::Key	Sì	Sì	Sì	Sì
AWS::Kinesis::Stream	Sì	Sì	Sì	No
AWS::Kinesis::StreamConsumer	Sì	Sì	Sì	No
AWS::KinesisAnalyticsV2::Application	Sì	Sì	Sì	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::KinesisFirehose::DeliveryStream	Sì	Sì	Sì	Sì
AWS::Lambda::CodeSigningConfig	Sì	Sì	No	No
AWS::Lambda::Function	Sì	Sì	Sì	Sì
AWS::Lex::Bot	No	Sì	No	No
AWS::Lex::BotAlias	No	Sì	No	No
AWS::Logs::Destination	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::MSK::BatchScramSegreto	Sì	Sì	Sì	No
AWS::MSK::Cluster	Sì	Sì	Sì	No
AWS::MSK::ClusterPolicy	Sì	Sì	Sì	Sì
AWS::MSK::Configuration	Sì	Sì	Sì	No
AWS::MSK::VpcConnection	Sì	Sì	Sì	Sì
AWS::MediaConnect::FlowEntitlement	No	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::MediaConnect::FlowSource	No	Sì	No	No
AWS::MediaConnect::FlowVpcInterfaccia	No	Sì	No	No
AWS::MediaTailor::PlaybackConfiguration	No	Sì	No	No
AWS::NetworkFirewall::Firewall	Sì	Sì	Sì	Sì
AWS::NetworkFirewall::FirewallPolicy	Sì	Sì	Sì	Sì
AWS::NetworkFirewall::RuleGroup	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::NetworkFirewall: :TLS InspectionConfiguration	Sì	Sì	Sì	Sì
AWS::OpenSearch::Domain	Sì	Sì	No	No
AWS::RDS::DBCluster	Sì	Sì	Sì	No
AWS: :RDS: :DB ClusterSnapshot	Sì	Sì	Sì	No
AWS::RDS::DBInstance	Sì	Sì	Sì	Sì
AWS: :RDS: :DB SecurityGroup	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::RDS::DBSnapshot	Sì	Sì	Sì	Sì
AWS: :RDS: :DB SubnetGroup	Sì	Sì	Sì	Sì
AWS::RDS::EventSubscription	Sì	Sì	Sì	Sì
AWS::RDS::OptionGroup	Sì	Sì	Sì	No
AWS::Redshift::Cluster	Sì	Sì	Sì	Sì
AWS::Redshift::ClusterParameterGruppo	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::Redshift::ClusterSecurityGruppo	Sì	Sì	Sì	Sì
AWS::Redshift::ClusterSnapshot	Sì	Sì	Sì	Sì
AWS::Redshift::ClusterSubnetGruppo	Sì	Sì	Sì	Sì
AWS::Redshift::EventSubscription	Sì	Sì	Sì	Sì
AWS::Redshift::ScheduledAction	Sì	No	No	No
AWS::ResilienceHub::App	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::ResilienceHub::ResiliencyPolicy	Sì	Sì	No	No
AWS::Route53Resolver::FirewallDomainElenco	Sì	Sì	No	No
AWS::Route53Resolver::FirewallRuleGruppo	Sì	Sì	No	No
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sì	Sì	No	No
AWS::Route53Resolver::ResolverEndpoint	Sì	Sì	Sì	No
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociazione	Sì	Sì	No	No
AWS::Route53Resolver::ResolverRule	Sì	Sì	Sì	No
AWS::Route53Resolver::ResolverRuleAssociazione	Sì	Sì	Sì	No
AWS::S3::AccessPoint	Sì	Sì	Sì	Sì
AWS::S3::AccountPublicAccessBlock	Sì	Sì	No	No
AWS::S3::Bucket	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::SES::ConfigurationSet	Sì	Sì	No	No
AWS::SES::ContactList	Sì	Sì	No	No
AWS::SES::Template	Sì	Sì	No	No
AWS::SNS::Topic	Sì	Sì	No	No
AWS::SQS::Queue	Sì	Sì	No	No
AWS::SSM::AssociationCompliance	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::SSM::Document	Sì	Sì	Sì	Sì
AWS::SSM::FileData	Sì	Sì	Sì	Sì
AWS::SSM::ManagedInstanceInventario	Sì	Sì	Sì	Sì
AWS::SSM::PatchCompliance	Sì	Sì	Sì	Sì
AWS::SageMaker::AppImageConfig	Sì	Sì	No	No
AWS::SageMaker::CodeRepository	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::SageMaker::Domain	Sì	Sì	No	No
AWS::SageMaker::EndpointConfig	Sì	Sì	No	No
AWS::SageMaker::FeatureGroup	Sì	Sì	No	No
AWS::SageMaker::Image	Sì	Sì	No	No
AWS::SageMaker::Model	Sì	Sì	No	No
AWS::SageMaker::NotebookInstance	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sì	Sì	No	No
AWS::SecretsManager::Secret	Sì	Sì	Sì	Sì
AWS::ServiceCatalog::CloudFormationProdotto	Sì	Sì	Sì	No
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sì	Sì	Sì	No
AWS::ServiceCatalog::Portfolio	Sì	Sì	Sì	No
AWS::ServiceDiscovery::HttpNamespace	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::ServiceDiscovery::Instance	Sì	Sì	Sì	No
AWS::ServiceDiscovery::PublicDnsNamespace	Sì	Sì	Sì	No
AWS::ServiceDiscovery::Service	Sì	Sì	Sì	No
AWS::ShieldRegional::Protection	Sì	Sì	Sì	No
AWS::Signer::SigningProfile	Sì	Sì	No	No
AWS::StepFunctions::Activity	Sì	Sì	Sì	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::StepFunctions::StateMachine	Sì	Sì	Sì	No
AWS::Transfer::Agreement	Sì	Sì	Sì	No
AWS::Transfer::Certificate	Sì	Sì	Sì	No
AWS::Transfer::Connector	Sì	Sì	Sì	No
AWS::Transfer::Profile	Sì	Sì	Sì	Sì
AWS::Transfer::Workflow	Sì	Sì	No	No

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::WAFRegional::RateBasedRegola	Sì	Sì	Sì	Sì
AWS::WAFRegional::Rule	Sì	Sì	Sì	Sì
AWS::WAFRegional::RuleGroup	Sì	Sì	Sì	Sì
AWS::WAFRegional::WebACL	Sì	Sì	Sì	Sì
AWS::WAFv2::IPSet	Sì	Sì	Sì	Sì
AWS::WAFv2::ManagedRuleImpostare	Sì	Sì	Sì	Sì

Tipo di risorsa	Africa (Città del Capo)	Medio Oriente (Bahrein)	Medio Oriente (Emirati Arabi Uniti)	Israele (Tel Aviv)
AWS::WAFv2::RegexPatternImpostare	Sì	Sì	Sì	Sì
AWS::WAFv2::RuleGroup	Sì	Sì	Sì	Sì
AWS::WAFv2::WebACL	Sì	Sì	Sì	Sì
AWS::WorkSpaces::Workspace	No	Sì	No	No
AWS::XRay::EncryptionConfig	No	Sì	Sì	Sì

GovCloud Regioni

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::ACM::Certificate	Sì	Sì
AWS::ACMPCA::CertificateAuthority	Sì	Sì
AWS::ACMPCA::CertificateAuthorityAttivazione	Sì	Sì
AWS::AccessAnalyzer::Analyzer	Sì	Sì
AWS::AmazonMQ::Broker	Sì	Sì
AWS::ApiGateway::RestApi	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::ApiGateway::Stage	Sì	Sì
AWS::ApiGatewayV2::Api	Sì	Sì
AWS::ApiGatewayV2::Stage	Sì	Sì
AWS::AppConfig::Application	Sì	Sì
AWS::AppConfig::ConfigurationProfile	Sì	Sì
AWS::AppConfig::DeploymentStrategy	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::AppConfig::Environment	Sì	Sì
AWS::AppConfig::ExtensionAssociation	Sì	Sì
AWS::AppConfig::HostedConfigurationVersione	Sì	Sì
AWS::AppStream::Application	Sì	Sì
AWS::AppStream::DirectoryConfig	No	Sì
AWS::AppStream::Fleet	No	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::AppStream::Stack	No	Sì
AWS::Athena::DataCatalog	Sì	Sì
AWS::Athena::WorkGroup	Sì	Sì
AWS::AutoScaling::AutoScalingGruppo	Sì	Sì
AWS::AutoScaling::LaunchConfiguration	Sì	Sì
AWS::AutoScaling::ScalingPolicy	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::AutoScaling::ScheduledAction	Sì	Sì
AWS::AutoScaling::WarmPool	Sì	Sì
AWS::Backup::BackupPlan	Sì	Sì
AWS::Backup::BackupSelection	Sì	Sì
AWS::Backup::BackupVault	Sì	Sì
AWS::Backup::RecoveryPoint	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::Batch::ComputeEnvironment	Sì	Sì
AWS::Batch::JobQueue	Sì	Sì
AWS::Batch::SchedulingPolicy	Sì	Sì
AWS::Cassandra::Keyspace	Sì	Sì
AWS::CloudFormation::Stack	Sì	Sì
AWS::CloudTrail::Trail	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::CloudWatch::Alarm	Sì	Sì
AWS::CodeBuild::Project	Sì	Sì
AWS::CodeBuild::ReportGroup	Sì	Sì
AWS::Cognito::UserPoolGruppo	No	Sì
AWS::Config::ConfigurationRecorder	Sì	Sì
AWS::Config::ConformancePackConformità	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::Config::ResourceCompliance	Sì	Sì
AWS::Connect::Instance	No	Sì
AWS::Connect::QuickConnect	No	Sì
AWS::DMS::Certificate	Sì	Sì
AWS::DMS::Endpoint	Sì	Sì
AWS::DMS::EventSubscription	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::DMS::ReplicationInstance	Sì	Sì
AWS::DMS::ReplicationSubnetGruppo	Sì	Sì
AWS::DMS::ReplicationTask	Sì	Sì
AWS::DataSync::LocationEFS	Sì	Sì
AWS::DataSync::LocationF SxLustre	Sì	Sì
AWS::DataSync::LocationF SxWindows	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::DataSync::LocationHDFS	Sì	Sì
AWS::DataSync::LocationNFS	Sì	Sì
AWS::DataSync::LocationObjectArchiviazione	Sì	Sì
AWS::DataSync::LocationS3	Sì	Sì
AWS::DataSync::LocationSMB	Sì	Sì
AWS::DataSync::Task	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::Detective::Graph	Sì	Sì
AWS::DynamoDB::Table	Sì	Sì
AWS::EC2::CapacityReservation	Sì	Sì
AWS::EC2::ClientVpnPunto finale	Sì	Sì
AWS::EC2::CustomerGateway	Sì	Sì
AWS::EC2::DHCPOptions	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::EC2::EC2Fleet	Sì	Sì
AWS::EC2::EIP	Sì	Sì
AWS::EC2::EgressOnlyInternetGateway	Sì	Sì
AWS::EC2::FlowLog	Sì	Sì
AWS::EC2::Host	Sì	Sì
AWS::EC2::IPAM	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::EC2::IPAMPool	Sì	Sì
AWS::EC2::IPAMScope	Sì	Sì
AWS::EC2::Instance	Sì	Sì
AWS::EC2::InternetGateway	Sì	Sì
AWS::EC2::LaunchTemplate	Sì	Sì
AWS::EC2::NatGateway	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::EC2::NetworkAcl	Sì	Sì
AWS::EC2::NetworkInterface	Sì	Sì
AWS::EC2::PrefixList	Sì	Sì
AWS::EC2::RouteTable	Sì	Sì
AWS::EC2::SecurityGroup	Sì	Sì
AWS::EC2::SpotFleet	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::EC2::Subnet	Sì	Sì
AWS::EC2::SubnetRouteTableAssociation	Sì	Sì
AWS::EC2::TrafficMirrorFiltro	Sì	Sì
AWS::EC2::TrafficMirrorSessione	Sì	Sì
AWS::EC2::TrafficMirrorObiettivo	Sì	Sì
AWS::EC2::TransitGateway	No	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::EC2::TransitGatewayAllegato	Sì	Sì
AWS::EC2::TransitGatewayConnect	Sì	Sì
AWS::EC2::TransitGatewayMulticastDomain	Sì	Sì
AWS::EC2::TransitGatewayRouteTable	Sì	Sì
AWS::EC2::VPC	Sì	Sì
AWS::EC2::VPCEndpoint	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS: :EC2: :VPC EndpointService	No	Sì
AWS: :EC2: :VPC PeeringConnection	Sì	Sì
AWS::EC2::VPNConnection	Sì	Sì
AWS::EC2::VPNGateway	Sì	Sì
AWS::EC2::Volume	Sì	Sì
AWS::ECR::Repository	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::ECS::CapacityProvider	Sì	Sì
AWS::ECS::Cluster	Sì	Sì
AWS::ECS::Service	Sì	Sì
AWS::ECS::TaskDefinition	Sì	Sì
AWS::ECS::TaskSet	Sì	Sì
AWS::EFS::AccessPoint	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::EFS::FileSystem	Sì	Sì
AWS::EKS::Addon	Sì	Sì
AWS::EKS::Cluster	Sì	Sì
AWS::EKS::IdentityProviderConfig	Sì	Sì
AWS::EMR::SecurityConfiguration	Sì	Sì
AWS::ElasticBeanstalk::Application	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::ElasticBeanstalk::ApplicationVersion	Sì	Sì
AWS::ElasticBeanstalk::Environment	Sì	Sì
AWS::ElasticLoadBalancing::LoadBalancer	Sì	Sì
AWS::ElasticLoadBalancingV2::Listener	Sì	Sì
AWS::ElasticLoadBalancingV2::LoadBalancer	Sì	Sì
AWS::Elasticsearch::Domain	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::Events::EventBus	Sì	Sì
AWS::Events::Rule	Sì	Sì
AWS::FIS::ExperimentTemplate	Sì	Sì
AWS::Glue::Classifier	Sì	Sì
AWS::Glue::Job	Sì	Sì
AWS::Glue:: MLTransform	No	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::GreengrassV2::ComponentVersion	Sì	Sì
AWS::GuardDuty::Detector	Sì	Sì
AWS::GuardDuty::Filter	Sì	Sì
AWS::GuardDovere: :IPSet	Sì	Sì
AWS::GuardDuty::ThreatIntelImpostare	Sì	Sì
AWS::IAM::Group	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::IAM::InstanceProfile	Sì	No
AWS::IAM::OIDCProvider	Sì	No
AWS::IAM::Policy	Sì	Sì
AWS::IAM::Role	Sì	Sì
AWS::IAM::SAMLProvider	Sì	No
AWS::IAM::ServerCertificate	Sì	No

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::IAM::User	Sì	Sì
AWS::ImageBuilder::ContainerRecipe	Sì	Sì
AWS::ImageBuilder::DistributionConfiguration	Sì	Sì
AWS::ImageBuilder::ImagePipeline	Sì	Sì
AWS::ImageBuilder::ImageRecipe	Sì	Sì
AWS::ImageBuilder::InfrastructureConfiguration	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::IoT::AccountAuditConfigurazione	Sì	Sì
AWS::IoT::Authorizer	Sì	Sì
AWS::IoCertificato T: :CA	Sì	Sì
AWS::IoT::CustomMetric	Sì	Sì
AWS::IoT::Dimension	Sì	Sì
AWS::IoT::FleetMetric	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::IoT::JobTemplate	Sì	Sì
AWS::IoT::MitigationAction	Sì	Sì
AWS::IoT::Policy	Sì	Sì
AWS::IoT::ProvisioningTemplate	Sì	Sì
AWS::IoT::RoleAlias	Sì	Sì
AWS::IoT::ScheduledAudit	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::IoT::SecurityProfile	Sì	Sì
AWS::IoTEvents::AlarmModel	No	Sì
AWS::IoTEvents::DetectorModel	No	Sì
AWS::IoTEvents::Input	No	Sì
AWS::IoTSiteWise::AssetModel	No	Sì
AWS::IoTSiteWise::Gateway	No	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::IoTSiteWise::Portal	No	Sì
AWS::IoTTwinMaker::ComponentType	No	Sì
AWS::IoTTwinMaker::Entity	No	Sì
AWS::IoTTwinMaker::Workspace	No	Sì
AWS::KMS::Alias	Sì	Sì
AWS::KMS::Key	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::Kinesis::Stream	Sì	Sì
AWS::Kinesis::StreamConsumer	Sì	Sì
AWS::KinesisAnalyticsV2::Application	Sì	Sì
AWS::KinesisFirehose::DeliveryStream	Sì	Sì
AWS::Lambda::Function	Sì	Sì
AWS::Logs::Destination	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::MSK::BatchScramSegreto	Sì	Sì
AWS::MSK::Cluster	Sì	Sì
AWS::MSK::ClusterPolicy	Sì	Sì
AWS::MSK::Configuration	Sì	Sì
AWS::MSK::VpcConnection	Sì	Sì
AWS::NetworkFirewall::Firewall	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::NetworkFirewall::FirewallPolicy	Sì	Sì
AWS::NetworkFirewall::RuleGroup	Sì	Sì
AWS::NetworkManager::CustomerGatewayAssociazione	No	Sì
AWS::NetworkManager::Device	No	Sì
AWS::NetworkManager::GlobalNetwork	No	Sì
AWS::NetworkManager::Link	No	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::NetworkManager::LinkAssociation	No	Sì
AWS::NetworkManager::Site	No	Sì
AWS::NetworkManager::TransitGatewayRegistrazione	No	Sì
AWS::OpenSearch::Domain	Sì	Sì
AWS::Pinpoint::App	No	Sì
AWS::Pinpoint::ApplicationSettings	No	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::Pinpoint::Campaign	No	Sì
AWS::Pinpoint::EmailChannel	No	Sì
AWS::Pinpoint::EmailTemplate	No	Sì
AWS::Pinpoint::EventStream	No	Sì
AWS::Pinpoint::InAppModello	No	Sì
AWS::Pinpoint::Segment	No	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::QuickSight::Template	No	Sì
AWS::RDS::DBCluster	Sì	Sì
AWS: :RDS: :DB ClusterSnapshot	Sì	Sì
AWS::RDS::DBInstance	Sì	Sì
AWS: :RDS: :DB SecurityGroup	Sì	Sì
AWS::RDS::DBSnapshot	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS: :RDS: :DB SubnetGroup	Sì	Sì
AWS::RDS::EventSubscription	Sì	Sì
AWS::RDS::OptionGroup	Sì	Sì
AWS::Redshift::Cluster	Sì	Sì
AWS::Redshift::ClusterParameterGruppo	Sì	Sì
AWS::Redshift::ClusterSecurityGruppo	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::Redshift::ClusterSnapshot	Sì	Sì
AWS::Redshift::ClusterSubnetGruppo	Sì	Sì
AWS::Redshift::EventSubscription	Sì	Sì
AWS::Redshift::ScheduledAction	Sì	Sì
AWS::RoboMaker::RobotApplication	No	Sì
AWS::RoboMaker::RobotApplicationVersione	No	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::RoboMaker::SimulationApplication	No	Sì
AWS::Route53Resolver::FirewallDomainElenco	Sì	Sì
AWS::Route53Resolver::FirewallRuleGruppo	Sì	Sì
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sì	Sì
AWS::Route53Resolver::ResolverEndpoint	Sì	Sì
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociazione	Sì	Sì
AWS::Route53Resolver::ResolverRule	Sì	Sì
AWS::Route53Resolver::ResolverRuleAssociazione	Sì	Sì
AWS::S3::AccessPoint	Sì	Sì
AWS::S3::AccountPublicAccessBlock	Sì	Sì
AWS::S3::Bucket	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::SES::ConfigurationSet	No	Sì
AWS::SES::ContactList	No	Sì
AWS::SES::Template	No	Sì
AWS::SNS::Topic	Sì	Sì
AWS::SQS::Queue	Sì	Sì
AWS::SSM::AssociationCompliance	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::SSM::Document	Sì	Sì
AWS::SSM::FileData	Sì	Sì
AWS::SSM::ManagedInstanceInventario	Sì	Sì
AWS::SSM::PatchCompliance	Sì	Sì
AWS::SageMaker::Model	No	Sì
AWS::SageMaker::NotebookInstance	No	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::SageMaker::NotebookInstanceLifecycleConfig	No	Sì
AWS::SecretsManager::Secret	Sì	Sì
AWS::ServiceCatalog::CloudFormationProdotto	Sì	Sì
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sì	Sì
AWS::ServiceCatalog::Portfolio	Sì	Sì
AWS::ServiceDiscovery::HttpNamespace	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::ServiceDiscovery::Instance	Sì	Sì
AWS::ServiceDiscovery::Service	Sì	Sì
AWS::StepFunctions::StateMachine	Sì	Sì
AWS::Transfer::Agreement	Sì	Sì
AWS::Transfer::Certificate	Sì	Sì
AWS::Transfer::Connector	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::Transfer::Profile	Sì	Sì
AWS::Transfer::Workflow	Sì	Sì
AWS::WAFRegional::RateBasedRegola	Sì	Sì
AWS::WAFRegional::Rule	Sì	Sì
AWS::WAFRegional::RuleGroup	Sì	Sì
AWS::WAFRegional::WebACL	Sì	Sì

Tipo di risorsa	AWS GovCloud (Stati Uniti occidentali)	AWS GovCloud (Stati Uniti orientali)
AWS::WAFv2::IPSet	Sì	Sì
AWS::WAFv2::ManagedRuleImpostare	Sì	Sì
AWS::WAFv2::RegexPatternImpostare	Sì	Sì
AWS::WAFv2::RuleGroup	Sì	Sì
AWS::WAFv2::WebACL	Sì	Sì
AWS::WorkSpaces::Workspace	No	Sì

AWS Risorse per la registrazione

AWS Config rileva continuamente quando i tipi di risorse supportati vengono creati, modificati o eliminati. AWS Config registra questi eventi come elementi di configurazione (CI). Puoi personalizzare AWS Config affinché registri le modifiche alla configurazione per tutti i tipi di risorse supportati o solo per i tipi di tuo interesse. Per un elenco dei tipi di risorse supportati che AWS Config possono registrare, vedereTipi di risorsa supportati.

Considerazioni

Numero elevato di AWS Config valutazioni

Potresti notare una maggiore attività nel tuo account durante la registrazione del mese iniziale con AWS Config rispetto ai mesi successivi. Durante il processo di avvio iniziale, AWS Config esegue valutazioni su tutte le risorse dell'account che hai selezionato per la AWS Config registrazione.

Se esegui carichi di lavoro temporanei, potresti riscontrare un aumento dell'attività dovuto alla registrazione delle modifiche alla configurazione associate alla creazione e all'eliminazione di queste risorse temporanee. AWS Config Un carico di lavoro temporaneo è un uso temporaneo di risorse di elaborazione che vengono caricate ed eseguite quando necessario. Tra gli esempi vi sono istanze spot di Amazon Elastic Compute Cloud (Amazon EC2), processi Amazon EMR e AWS Auto Scaling. Se desideri evitare l'aumento dell'attività dovuto all'esecuzione di carichi di lavoro temporanei, puoi configurare il registratore di configurazione in modo da escludere questi tipi di risorse dalla registrazione oppure eseguire questi tipi di carichi di lavoro in un account separato con AWS Config l'opzione disattivata per evitare un aumento della registrazione della configurazione e delle valutazioni delle regole.

Disponibilità nelle Regioni

Prima di specificare un tipo di risorsa da AWS Config monitorare, verifica la disponibilità della copertura delle risorse per regione per vedere se il tipo di risorsa è supportato nella regione in cui è stato configurato. AWS AWS Config Se un tipo di risorsa è supportato da AWS Config almeno una regione, puoi abilitare la registrazione di quel tipo di risorsa in tutte le regioni supportate da AWS Config, anche se il tipo di risorsa specificato non è supportato nella AWS regione in cui è stato configurato AWS Config.

Quali sono le differenze tra risorse regionali e globali?

Risorse regionali

Le risorse regionali sono legate a una regione e possono essere utilizzate solo in tale regione. Le crei in una determinata Regione AWS regione e quindi esistono in quella regione. Per visualizzare o interagire con tali risorse, occorre indirizzare le tue operazioni verso quella regione. Ad esempio, per creare un'istanza Amazon EC2 con AWS Management Console, scegli l'istanza in Regione AWS cui desideri creare l'istanza. Se usi AWS Command Line Interface (AWS CLI) per creare l'istanza, includi il `--region` parametro. Ciascuno degli AWS SDK dispone di un proprio meccanismo equivalente per specificare la regione utilizzata dall'operazione.

Esistono diversi motivi per utilizzare le risorse regionali. Uno di questi è garantire che le risorse e gli endpoint di servizio utilizzati per accedervi siano il più vicino possibile al cliente. Ciò migliora le prestazioni riducendo al minimo la latenza. Un altro motivo è quello di fornire un limite di isolamento. Ciò consente di creare copie indipendenti delle risorse in più regioni per distribuire il carico e migliorare la scalabilità. Allo stesso tempo, le risorse sono isolate l'una dall'altra per migliorare la disponibilità.

Se ne specifichi una diversa Regione AWS nella console o in un AWS CLI comando, non potrai più vedere o interagire con le risorse che potevi vedere nella regione precedente.

Esaminando il nome della risorsa Amazon (ARN) di una risorsa regionale, la regione in cui si trova la risorsa è specificata nel quarto campo dell'ARN. Ad esempio, un'istanza Amazon EC2 è una risorsa regionale. Di seguito è riportato un esempio di un ARN di un'istanza Amazon EC2 nella regione `us-east-1`.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

Risorse globali

Alcune risorse di AWS servizi sono risorse globali, il che significa che è possibile utilizzare la risorsa da qualsiasi luogo. Nella console di un servizio globale, non occorre specificare una Regione AWS . Per accedere a una risorsa globale, non è necessario specificare un `--region` parametro quando si utilizzano le operazioni del servizio AWS CLI e dell' AWS SDK.

Le risorse globali supportano i casi in cui è fondamentale che possa esistere solo un'istanza di una particolare risorsa alla volta. In questi scenari, la replica o la sincronizzazione tra copie in regioni diverse non è adeguata. La necessità di accedere a un unico endpoint globale, con il

possibile aumento della latenza, è considerata accettabile per garantire che eventuali modifiche siano immediatamente visibili ai consumatori della risorsa.

Ad esempio, i cluster globali di Amazon Aurora (`AWS::RDS::GlobalCluster`) sono risorse globali e quindi non sono legati a una regione. Ciò significa che puoi creare un cluster globale senza fare affidamento su un endpoint regionale. Il vantaggio è che, mentre lo stesso Amazon Relational Database Service (Amazon RDS) è organizzato per regioni, la regione specifica in cui ha origine un cluster globale non influisce su quest'ultimo, che si presenta come un unico cluster globale continuo in tutte le regioni.

Il nome della risorsa Amazon (ARN) di una risorsa globale non include la regione. Il quarto campo è vuoto, come nell'esempio seguente di ARN di un cluster globale.

```
arn:aws:rds::123456789012:global-cluster:test-global-cluster
```

> **Important**
>
> I tipi di risorse globali registrati AWS Config dopo febbraio 2022 verranno registrati solo nella regione di origine del servizio per la partizione commerciale e AWS GovCloud (Stati Uniti occidentali) per la partizione. GovCloud È possibile visualizzare gli elementi di configurazione (CI) per questi nuovi tipi di risorse globali solo nella loro regione di origine e (Stati Uniti occidentali). AWS GovCloud
> I tipi di risorse globali introdotti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy` `AWS::IAM::Role` e `AWS::IAM::User`) rimangono invariati. Puoi abilitare la registrazione di queste risorse IAM globali in tutte le regioni in cui AWS Config era supportata prima di febbraio 2022. Queste risorse IAM globali non possono essere registrate nelle regioni supportate AWS Config dopo febbraio 2022.

Tipi di risorse globali | Risorse IAM

Anche i seguenti tipi di risorse IAM sono risorse a livello globale: utenti IAM, gruppi, ruoli e policy gestite dal cliente. Questi tipi di risorse possono essere registrati AWS Config nelle regioni in cui AWS Config erano disponibili prima di febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.

Per evitare la duplicazione degli elementi di configurazione (CI), dovresti prendere in considerazione la registrazione dei tipi di risorse IAM globali una sola volta in una delle regioni

supportate. Questo può anche aiutarti a evitare valutazioni non necessarie e limitazioni delle API.

Tipi di risorse globali | Solo area geografica

Le risorse globali per i seguenti servizi vengono registrate solo AWS Config nella regione di origine del tipo di risorsa globale: Amazon Elastic Container Registry Public AWS Global Accelerator, Amazon Route 53 CloudFront, Amazon e AWS WAF. Per queste risorse globali, la stessa istanza del tipo di risorsa può essere utilizzata in più AWS regioni, ma gli elementi di configurazione (CI) vengono registrati solo nella regione di origine per la partizione commerciale o AWS GovCloud (Stati Uniti occidentali) per la partizione. AWS GovCloud (US)

Regioni di origine dei tipi di risorse globali

AWS Servizio	Valore tipo di risorsa	Regione di origine
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	Stati Uniti orientali (Virginia settentrionale)
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	Stati Uniti occidentali (Oregon)
	`AWS::GlobalAccelerator::EndpointGroup`	Stati Uniti occidentali (Oregon)
	`AWS::GlobalAccelerator::Accelerator`	Stati Uniti occidentali (Oregon)
Amazon Route 53	`AWS::Route53::HostedZone`	Stati Uniti orientali (Virginia settentrionale)
	`AWS::Route53::HealthCheck`	Stati Uniti orientali (Virginia settentrionale)
Amazon CloudFront	`AWS::CloudFront::Distribution`	Stati Uniti orientali (Virginia settentrionale)
AWS WAF	`AWS::WAFv2::WebACL`	Stati Uniti orientali (Virginia settentrionale)

Tipi di risorse globali | Cluster globali Aurora

`AWS::RDS::GlobalClusterè` una risorsa globale registrata in tutte le AWS Config regioni supportate in cui è abilitato il registratore di configurazione. Questo tipo di risorsa globale è unico in quanto, se abiliti la registrazione di questa risorsa in una regione, AWS Config registrerà gli elementi di configurazione (CI) per questo tipo di risorsa in tutte le regioni abilitate.

Se non desiderate registrare `AWS::RDS::GlobalCluster` in tutte le regioni abilitate, utilizzate una delle seguenti strategie di registrazione per la AWS Config console:

- Registra tutti i tipi di risorse con sostituzioni personalizzabili, scegli "AWS RDS GlobalCluster «e scegli l'opzione alternativa «Escludi dalla registrazione»
- Registra tipi di risorsa specifici.

Se non desideri registrare `AWS::RDS::GlobalCluster` in tutte le regioni abilitate, utilizza una delle seguenti strategie di registrazione per API/CLI:

- Registra tutti i tipi di risorse attuali e futuri con esclusioni (`EXCLUSION_BY_RESOURCE_TYPES`)
- Registra tipi di risorsa specifici (`INCLUSION_BY_RESOURCE_TYPES`).

Risorse di registrazione nella console AWS Config

Risorse di registrazione (Console)

È possibile utilizzare la AWS Config console per selezionare i tipi di risorse da AWS Config registrare.

Per scegliere le risorse

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Nella barra di navigazione a sinistra, scegli Impostazioni e successivamente Modifica. Per l'elenco delle regioni supportate, consulta Endpoint e quote AWS Config in Riferimenti generali di Amazon Web Services.
3. Nella sezione Metodo di registrazione, scegli una strategia di registrazione. È possibile specificare le AWS risorse che si AWS Config desidera registrare.

All resource types with customizable overrides

Imposta AWS Config per registrare le modifiche alla configurazione per tutti i tipi di risorse supportati attuali e futuri in questa regione. È possibile sovrascrivere la frequenza di registrazione per tipi di risorse specifici o escludere tipi di risorse specifici dalla registrazione. Per ulteriori informazioni, consulta Tipi di risorsa supportati.

- Impostazioni predefinite

  Configura la frequenza di registrazione predefinita per tutti i tipi di risorse supportate attuali e future. Per ulteriori informazioni, vedere Frequenza di registrazione.

  - Registrazione continua: AWS Config registrerà le modifiche alla configurazione in modo continuo ogni volta che si verifica una modifica.
  - La registrazione giornaliera consente di ricevere un elemento di configurazione (CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza.

  > **Note**
  >
  > AWS Firewall Manager dipende dalla registrazione continua per monitorare le risorse. Se si utilizza Firewall Manager, si consiglia di impostare la frequenza di registrazione su Continuo.

- Sostituzione delle impostazioni

  Sostituisci la frequenza di registrazione per tipi di risorse specifici o escludi tipi di risorse specifici dalla registrazione. Se cambi la frequenza di registrazione per un tipo di risorsa o interrompi la registrazione per un tipo di risorsa, gli elementi della configurazione già registrati rimarranno invariati.

  > **Note**
  >
  > Tipi di risorse globali | I cluster globali Aurora sono inizialmente inclusi nella registrazione
  > Il tipo di `AWS::RDS::GlobalCluster` risorsa verrà registrato in tutte le AWS Config regioni supportate in cui è abilitato il registratore di configurazione.

Se non desideri registrare `AWS::RDS::GlobalCluster` in tutte le regioni abilitate, scegli "AWS RDS GlobalCluster“ e scegli l'opzione alternativa “Escludi dalla registrazione”.

> **Note**
>
> Tipi di risorse globali | I tipi di risorse IAM sono inizialmente esclusi dalla registrazione
>
> “Tutti i tipi di risorse IAM registrati a livello globale” sono inizialmente esclusi dalla registrazione per aiutarti a ridurre i costi. Questo pacchetto include gli utenti IAM, i gruppi, i ruoli e le policy gestite dal cliente. Scegli Rimuovi per rimuovere l'override e includere queste risorse nella registrazione.
>
> L'eccezione a questa nota è per gli Stati Uniti orientali (Virginia settentrionale). I tipi di risorse IAM globali sono inizialmente inclusi nella regione Stati Uniti orientali (Virginia settentrionale) poiché questa regione funge da regione principale per i tipi di risorse IAM globali.
>
> Inoltre, i tipi di risorse IAM globali (`AWS::IAM::User`,`AWS::IAM::Group`,`AWS::IAM::Role`, e`AWS::IAM::Policy`) non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta Recording AWS Resources | Global Resources.

> **Note**
>
> Limiti
>
> È possibile aggiungere fino a 100 sostituzioni di frequenza e 600 sostituzioni di esclusione.
>
> La registrazione giornaliera non è supportata per i tipi di risorse seguenti:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Specific resource types

Imposta AWS Config per registrare le modifiche alla configurazione solo per i tipi di risorse specificati.

- Tipi di risorsa specifici

  Scegli un tipo di risorsa da registrare e la relativa frequenza. Per ulteriori informazioni, vedere Frequenza di registrazione.

  - Registrazione continua: AWS Config registrerà le modifiche alla configurazione in modo continuo ogni volta che si verifica una modifica.
  - La registrazione giornaliera consente di ricevere un elemento di configurazione (CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza.

  > **Note**
  >
  > AWS Firewall Manager dipende dalla registrazione continua per monitorare le risorse. Se si utilizza Firewall Manager, si consiglia di impostare la frequenza di registrazione su Continuo.

  Se cambi la frequenza di registrazione per un tipo di risorsa o interrompi la registrazione per un tipo di risorsa, gli elementi della configurazione già registrati rimarranno invariati.

> **Note**
>
> Disponibilità nelle Regioni
> Prima di specificare un tipo di risorsa da AWS Config monitorare, verifica la disponibilità della copertura delle risorse per regione per vedere se il tipo di risorsa è supportato nella AWS regione in cui è stato configurato AWS Config. Se un tipo di risorsa è supportato da AWS Config almeno una regione, puoi abilitare la registrazione di quel tipo di risorsa in tutte le regioni supportate da AWS Config, anche se il tipo di risorsa specificato non è supportato nella AWS regione in cui è stato configurato AWS Config.

> **Note**
>
> Limiti
>
> Nessun limite se tutti i tipi di risorse hanno la stessa frequenza. È possibile aggiungere fino a 100 tipi di risorse con frequenza giornaliera se almeno un tipo di risorsa è impostato su Continuo.
>
> La frequenza giornaliera non è supportata per i tipi di risorse seguenti:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

4. Scegliere Salva per salvare le modifiche.

Risorse di registrazione con la AWS CLI

Risorse di registrazione (AWS CLI)

È possibile utilizzare la AWS CLI per selezionare i tipi di risorse che si desidera AWS Config registrare. Per farlo devi creare un registratore di configurazione, che registra i tipi di risorse che specifichi in un gruppo di registrazione. Nel gruppo di registrazione, specifica se desideri registrare tutti i tipi di risorse supportati o se desideri includere o escludere tipi di risorse specifici.

Record all current and future supported resource types

Imposta AWS Config per registrare le modifiche alla configurazione per tutti i tipi di risorse supportati attuali e futuri in questa regione. Per ulteriori informazioni, consulta Tipi di risorsa supportati.

1. Utilizzando il seguente comando `put-configuration-recorder`:

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

Questo comando utilizza i `---recording-group` campi `--configuration-recorder` and.

> **Note**
>
> Gruppo di registrazione e registratore di configurazione
> Il campo `--recording-group` specifica quali tipi di risorse vengono registrati.
> Il `--configuration-recorder` campo specifica `name` e la frequenza `roleArn` di registrazione predefinita per il registratore di configurazione (). `recordingMode` È inoltre possibile utilizzare questo campo per sovrascrivere la frequenza di registrazione per tipi di risorse specifici.

i. `put-configuration-recorder` usa i seguenti campi per il parametro `--recording-group`:

- `allSupported=true`— AWS Config registra le modifiche alla configurazione per tutti i tipi di risorse supportati, esclusi i tipi di risorse IAM globali. Quando AWS Config aggiunge il supporto per un nuovo tipo di risorsa, AWS Config inizia a registrare automaticamente le risorse di quel tipo.
- `includeGlobalResourceTypes=true`: questa opzione è un bundle che si applica solo ai tipi di risorse IAM registrati a livello globale: utenti IAM, gruppi, ruoli e policy gestite dal cliente. Questi tipi di risorse IAM globali possono essere registrati solo AWS Config nelle regioni in cui AWS Config erano disponibili prima di febbraio 2022. Non è possibile registrare i tipi di risorse IAM globali nelle regioni supportate AWS Config entro febbraio 2022. Per un elenco di tali regioni, consulta Recording AWS Resources | Global Resources.

> **Important**
>
> I cluster globali Aurora sono registrati in tutte le regioni abilitate
> Il tipo di `AWS::RDS::GlobalCluster` risorsa verrà registrato in tutte le AWS Config regioni supportate in cui il registratore di configurazione è abilitato, anche se non `includeGlobalResourceTypes` è impostato `true` su. L'opzione `includeGlobalResourceTypes` è un pacchetto applicabile solo agli utenti IAM, ai gruppi, ai ruoli e alle policy gestite dal cliente.
> Se non desideri registrare `AWS::RDS::GlobalCluster` in tutte le regioni abilitate, utilizza una delle seguenti strategie di registrazione:

1. Registra tutti i tipi di risorse attuali e futuri esclusi i tipi che specifichi (`EXCLUSION_BY_RESOURCE_TYPES`) o
2. Registra tipi di risorsa specifici (`INCLUSION_BY_RESOURCE_TYPES`).

Per ulteriori informazioni, consulta Scegli quali risorse devono essere registrate | Risorse regionali e globali.

Important

strategia di GlobalResourceTypes registrazione di inclusione ed esclusione
Il `includeGlobalResourceTypes` campo non ha alcun impatto sulla strategia `EXCLUSION_BY_RESOURCE_TYPES` di registrazione. Ciò significa che i tipi di risorse IAM globali (utenti IAM, gruppi, ruoli e policy gestite dai clienti) non verranno aggiunti automaticamente come esclusioni per `exclusionByResourceTypes` quando `includeGlobalResourceTypes` è impostato su. `false`
Il `includeGlobalResourceTypes` campo deve essere utilizzato solo per modificare il `AllSupported` campo, poiché l'impostazione predefinita per il `AllSupported` campo consiste nel registrare le modifiche alla configurazione per tutti i tipi di risorse supportati, esclusi i tipi di risorse IAM globali. Per includere i tipi di risorse IAM globali quando `AllSupported` è impostato su`true`, assicurati di `includeGlobalResourceTypes` impostarlo su`true`.
Per escludere i tipi di risorse IAM globali per la strategia di `EXCLUSION_BY_RESOURCE_TYPES` registrazione, devi aggiungerli manualmente al `resourceTypes` campo di`exclusionByResourceTypes`.

Note

Campi obbligatori e facoltativi
Prima di impostare `includeGlobalResourceTypes` su `true`, imposta il campo `allSupported` su `true`.
Facoltativamente, puoi anche impostare il campo `useOnly` di `RecordingStrategy` su `ALL_SUPPORTED_RESOURCE_TYPES`.

> **Note**
>
> Sostituzione dei campi
>
> Se `includeGlobalResourceTypes` imposti su `false` ma elenchi i tipi di risorse IAM globali nel `resourceTypes` campo di RecordingGroup, AWS Config registrerà comunque le modifiche alla configurazione per quei tipi di risorse specificati indipendentemente dal fatto che il `includeGlobalResourceTypes` campo sia impostato su false.
>
> Se non desideri registrare le modifiche alla configurazione dei tipi di risorse IAM registrati a livello globale (policy gestite dal cliente o da gruppi, ruoli e utenti IAM), assicurati di non elencarli nel campo `resourceTypes` e di impostare il campo `includeGlobalResourceTypes` su false.

Il file `recordingGroup.json` specifica quali tipi di risorse saranno registrati da AWS Config .

```
{
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

ii. `put-configuration-recorder` usa i seguenti campi per il parametro `--configuration-recorder`:

- `name`— Il nome del registratore di configurazione. AWS Config assegna automaticamente il nome di «default» durante la creazione del registratore di configurazione.
- `roleARN`— Amazon Resource Name (ARN) del ruolo IAM assunto AWS Config e utilizzato dal registratore di configurazione.
- `recordingMode`— Speciifica la frequenza di registrazione predefinita AWS Config utilizzata per registrare le modifiche alla configurazione. AWS Config supporta la registrazione continua e la registrazione giornaliera. La registrazione continua consente di registrare continuamente le modifiche alla configurazione ogni volta che si verifica una modifica. La registrazione giornaliera consente di ricevere un elemento di configurazione

(CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza.

- `recordingFrequency`— La frequenza di registrazione predefinita AWS Config utilizzata per registrare le modifiche alla configurazione.

> **Note**
>
> AWS Firewall Manager dipende dalla registrazione continua per monitorare le risorse. Se si utilizza Firewall Manager, si consiglia di impostare la frequenza di registrazione su Continuo.

- `recordingModeOverrides`: questo campo consente di specificare le sostituzioni per la modalità di registrazione. Si tratta di un array di oggetti `recordingModeOverride`. Ogni oggetto `recordingModeOverride` dell'array `recordingModeOverrides` è composto da tre campi:
  - `description`— Una descrizione fornita per l'override.
  - `recordingFrequency`— La frequenza di registrazione che verrà applicata a tutti i tipi di risorse specificati nell'override.
  - `resourceTypes`— Un elenco separato da virgole che specifica quali tipi di risorse sono AWS Config inclusi nell'override.

> **Note**
>
> Campi obbligatori e facoltativi
>
> Il campo `recordingMode` per `put-configuration-recorder` è facoltativo. Per impostazione predefinita, la frequenza di registrazione per il registratore di configurazione è impostata su Registrazione continua.

> **Note**
>
> Limiti
>
> La registrazione giornaliera non è supportata per i tipi di risorse seguenti:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Per la strategia di registrazione Registra tutti i tipi di risorse supportati attuali e futuri (`ALL_SUPPORTED_RESOURCE_TYPES`), questi tipi di risorse saranno impostati su Registrazione continua.

Il `configurationRecorder.json` file specifica `name` e `roleArn` la frequenza di registrazione predefinita per il registratore di configurazione (). `recordingMode` È inoltre possibile utilizzare questo campo per sovrascrivere la frequenza di registrazione per tipi di risorse specifici.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to
 include in the override ]
        }
    ]
  }
}
```

2. (Facoltativo) Per verificare se il registratore di configurazione è impostato come desiderato, utilizza il seguente comando `describe-configuration-recorders`.

```
$ aws configservice describe-configuration-recorders
```

Di seguito è riportata una risposta di esempio.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default"
            "recordingGroup": {
                "allSupported": true,
                "exclusionByResourceTypes": {
                     "resourceTypes": []
```

```
                },
                "includeGlobalResourceTypes": true,
                "recordingStrategy": {
                    "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types
 to include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record all current and future supported resources types excluding the types you specify

Imposta per registrare le modifiche AWS Config alla configurazione per tutti i tipi di risorse supportati attuali e futuri, inclusi i tipi di risorse globali, ad eccezione dei tipi di risorse che hai specificato di escludere dalla registrazione. Se scegli di interrompere la registrazione per un tipo di risorsa, gli elementi della configurazione già registrati rimarranno invariati. Per ulteriori informazioni, consulta Tipi di risorsa supportati.

Questo comando utilizza i `---recording-group` campi `--configuration-recorder` and.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

> **Note**
>
> Gruppo di registrazione e registratore di configurazione
>
> Il campo `--recording-group` specifica quali tipi di risorse vengono registrati.

Il `--configuration-recorder` campo specifica `name` e la frequenza `roleArn` di registrazione predefinita per il registratore di configurazione (). `recordingMode` È inoltre possibile utilizzare questo campo per sovrascrivere la frequenza di registrazione per tipi di risorse specifici.

1. Utilizza il comando `put-configuration-recorder` e trasmetti uno o più tipi di risorse da escludere nel campo `resourceTypes` di `exclusionByResourceTypes`, come mostrato nell'esempio seguente.
   i. Il file `recordingGroup.json` specifica quali tipi di risorse saranno registrati da AWS Config .

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
            "AWS::CloudFront::StreamingDistribution"
        ]
    },
   "includeGlobalResourceTypes": false,
   "recordingStrategy": {
       "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
    },

}
```

   Prima di specificare i tipi di risorse da escludere dalla registrazione:

   - È necessario impostare i campi `allSupported` e `includeGlobalResourceTypes` del parametro `--recording-group` su `false` oppure ometterli.
   - È necessario impostare il campo `useOnly` di `RecordingStrategy` su `EXCLUSION_BY_RESOURCE_TYPES`.

> **Note**
>
> Sostituzione dei campi
>
> Se scegli `EXCLUSION_BY_RESOURCE_TYPES` come strategia di registrazione, il campo `exclusionByResourceTypes` sovrascrive le altre proprietà della richiesta.

Ad esempio, anche se hai impostato `includeGlobalResourceTypes` su false, i tipi di risorse IAM registrati a livello globale verranno comunque registrati automaticamente in questa opzione, a meno che tali tipi di risorse non siano specificamente elencati come esclusioni nel campo `resourceTypes` di `exclusionByResourceTypes`.

> **Note**
>
> Tipi di risorse globali e strategia di registrazione di esclusione delle risorse
> Per impostazione predefinita, se si sceglie la strategia di `EXCLUSION_BY_RESOURCE_TYPES` registrazione, When AWS Config aggiunge il supporto per un nuovo tipo di risorsa nella regione in cui è impostato il registratore di configurazione, inclusi i tipi di risorse globali, AWS Config avvia automaticamente la registrazione di risorse di quel tipo.
> A meno che non siano specificatamente elencate come esclusioni, `AWS::RDS::GlobalCluster` verranno registrate automaticamente in tutte le AWS Config regioni supportate in cui il registratore di configurazione è abilitato.
> Gli utenti, i gruppi, i ruoli e le politiche gestite dai clienti di IAM verranno registrati nella regione in cui è stato configurato il registratore di configurazione, se questa è una regione in cui AWS Config era disponibile prima di febbraio 2022. Non puoi registrare i tipi di risorse IAM globali nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta Recording AWS Resources | Global Resources.

ii. `put-configuration-recorder` usa i seguenti campi per il parametro `--configuration-recorder`:

- `name`— Il nome del registratore di configurazione. AWS Config assegna automaticamente il nome di «default» durante la creazione del registratore di configurazione.
- `roleARN`— Amazon Resource Name (ARN) del ruolo IAM assunto AWS Config e utilizzato dal registratore di configurazione.
- `recordingMode`— Speciifica la frequenza di registrazione predefinita AWS Config utilizzata per registrare le modifiche alla configurazione. AWS Config supporta la registrazione continua e la registrazione giornaliera. La registrazione continua consente di registrare continuamente le modifiche alla configurazione ogni volta che si verifica una modifica. La registrazione giornaliera consente di ricevere un elemento di configurazione

(CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza.

- `recordingFrequency`— La frequenza di registrazione predefinita AWS Config utilizzata per registrare le modifiche alla configurazione.

> **Note**
>
> AWS Firewall Manager dipende dalla registrazione continua per monitorare le risorse. Se si utilizza Firewall Manager, si consiglia di impostare la frequenza di registrazione su Continuo.

- `recordingModeOverrides`: questo campo consente di specificare le sostituzioni per la modalità di registrazione. Si tratta di un array di oggetti `recordingModeOverride`. Ogni oggetto `recordingModeOverride` dell'array `recordingModeOverrides` è composto da tre campi:
  - `description`— Una descrizione fornita per l'override.
  - `recordingFrequency`— La frequenza di registrazione che verrà applicata a tutti i tipi di risorse specificati nell'override.
  - `resourceTypes`— Un elenco separato da virgole che specifica quali tipi di risorse sono AWS Config inclusi nell'override.

> **Note**
>
> Campi obbligatori e facoltativi
>
> Il campo `recordingMode` per `put-configuration-recorder` è facoltativo. Per impostazione predefinita, la frequenza di registrazione per il registratore di configurazione è impostata su Registrazione continua.

> **Note**
>
> Limiti
>
> La registrazione giornaliera non è supportata per i tipi di risorse seguenti:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Per la strategia di registrazione Registra tutti i tipi di risorse supportati attuali e futuri (`ALL_SUPPORTED_RESOURCE_TYPES`), questi tipi di risorse saranno impostati su Registrazione continua.

Il `configurationRecorder.json` file specifica `name` e `roleArn` la frequenza di registrazione predefinita per il registratore di configurazione (). `recordingMode` È inoltre possibile utilizzare questo campo per sovrascrivere la frequenza di registrazione per tipi di risorse specifici.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to
 include in the override ]
        }
    ]
  }
}
```

2. (Facoltativo) Per verificare se il registratore di configurazione è impostato come desiderato, utilizza il seguente comando `describe-configuration-recorders`.

```
$ aws configservice describe-configuration-recorders
```

Di seguito è riportata una risposta di esempio.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
```

```
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
                "recordingStrategy": {
                    "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record specific resource types

Imposta AWS Config per registrare le modifiche alla configurazione solo per i tipi di risorse specificati. Se scegli di interrompere la registrazione per un tipo di risorsa, gli elementi della configurazione già registrati rimarranno invariati.

Questo comando utilizza i `---recording-group` campi `--configuration-recorder` and.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

> **Note**
>
> Gruppo di registrazione e registratore di configurazione

Il campo `--recording-group` specifica quali tipi di risorse vengono registrati.
Il `--configuration-recorder` campo specifica `name` e la frequenza `roleArn` di registrazione predefinita per il registratore di configurazione (). `recordingMode` È inoltre possibile utilizzare questo campo per sovrascrivere la frequenza di registrazione per tipi di risorse specifici.

1. Utilizza il comando `put-configuration-recorder` e trasmetti uno o più tipi di risorse nel campo `resourceTypes` di `recordingGroup`, come mostrato nell'esempio seguente.
   i. Il file `recordingGroup.json` specifica quali tipi di risorse saranno registrati da AWS Config .

```
{
    "allSupported": false,
    "recordingStrategy": {
        "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": false,
    "resourceTypes": [
        "AWS::EC2::EIP",
        "AWS::EC2::Instance",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::SecurityGroup",
        "AWS::CloudTrail::Trail",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC",
        "AWS::IAM::User",
        "AWS::IAM::Policy"
  ]
}
```

> **Note**
>
> Campi obbligatori e facoltativi
> Prima di specificare i tipi di risorse da includere nella registrazione, è necessario impostare i campi `allSupported` e `includeGlobalResourceTypes` su `false` oppure ometterli.

Il campo `recordingStrategy` è facoltativo se elenchi i tipi di risorse nel campo `resourceTypes` di `--recording-group`.

> **Note**
>
> Disponibilità nelle Regioni
>
> Prima di specificare un tipo di risorsa da AWS Config tracciare, controllate la disponibilità della copertura delle risorse per regione per vedere se il tipo di risorsa è supportato nella AWS regione in cui è stato configurato. AWS Config Se un tipo di risorsa è supportato da AWS Config almeno una regione, puoi abilitare la registrazione di quel tipo di risorsa in tutte le regioni supportate da AWS Config, anche se il tipo di risorsa specificato non è supportato nella AWS regione in cui è stato configurato AWS Config.

ii. `put-configuration-recorder` usa i seguenti campi per il parametro `--configuration-recorder`:

- `name`— Il nome del registratore di configurazione. AWS Config assegna automaticamente il nome di «default» durante la creazione del registratore di configurazione.
- `roleARN`— Amazon Resource Name (ARN) del ruolo IAM assunto AWS Config e utilizzato dal registratore di configurazione.
- `recordingMode`— Speciifica la frequenza di registrazione predefinita AWS Config utilizzata per registrare le modifiche alla configurazione. AWS Config supporta la registrazione continua e la registrazione giornaliera. La registrazione continua consente di registrare continuamente le modifiche alla configurazione ogni volta che si verifica una modifica. La registrazione giornaliera consente di ricevere un elemento di configurazione (CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza.
  - `recordingFrequency`— La frequenza di registrazione predefinita AWS Config utilizzata per registrare le modifiche alla configurazione.

> **Note**
>
> AWS Firewall Manager dipende dalla registrazione continua per monitorare le risorse. Se si utilizza Firewall Manager, si consiglia di impostare la frequenza di registrazione su Continuo.

- `recordingModeOverrides`: questo campo consente di specificare le sostituzioni per la modalità di registrazione. Si tratta di un array di oggetti `recordingModeOverride`. Ogni oggetto `recordingModeOverride` dell'array `recordingModeOverrides` è composto da tre campi:
  - `description`— Una descrizione fornita per l'override.
  - `recordingFrequency`— La frequenza di registrazione che verrà applicata a tutti i tipi di risorse specificati nell'override.
  - `resourceTypes`— Un elenco separato da virgole che specifica quali tipi di risorse sono AWS Config inclusi nell'override.

> **Note**
>
> Campi obbligatori e facoltativi
>
> Il campo `recordingMode` per `put-configuration-recorder` è facoltativo. Per impostazione predefinita, la frequenza di registrazione per il registratore di configurazione è impostata su Registrazione continua.

> **Note**
>
> Limiti
>
> La registrazione giornaliera non è supportata per i tipi di risorse seguenti:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> Per la strategia di registrazione Registra tutti i tipi di risorse supportati attuali e futuri (`ALL_SUPPORTED_RESOURCE_TYPES`), questi tipi di risorse saranno impostati su Registrazione continua.

Il `configurationRecorder.json` file specifica `name` e `roleArn` la frequenza di registrazione predefinita per il registratore di configurazione (). `recordingMode` È inoltre possibile utilizzare questo campo per sovrascrivere la frequenza di registrazione per tipi di risorse specifici.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to
 include in the override ]
        }
    ]
  }
}
```

2. (Facoltativo) Per verificare se il registratore di configurazione è impostato come desiderato, utilizza il seguente comando `describe-configuration-recorders`.

```
$ aws configservice describe-configuration-recorders
```

Di seguito è riportata una risposta di esempio.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": []
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
```

```
                },
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Frequenza registrazione

AWS Config supporta la registrazione continua e la registrazione giornaliera. La registrazione continua consente di registrare continuamente le modifiche alla configurazione ogni volta che si verifica una modifica. La registrazione giornaliera consente di ricevere un elemento di configurazione (CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza.

Registrazione continua

Alcuni dei vantaggi derivanti dalla registrazione continua sono:

- Monitoraggio in tempo reale: la registrazione continua può fornire il rilevamento immediato di modifiche non autorizzate o alterazioni impreviste, il che può migliorare gli sforzi in materia di sicurezza e conformità.
- Analisi dettagliata: la registrazione continua consente di eseguire un'analisi approfondita delle modifiche alla configurazione delle risorse man mano che si verificano, il che può consentire di identificare modelli e tendenze del momento.

Registrazione giornaliera

Alcuni dei vantaggi derivanti dalla registrazione giornaliera sono:

- Interruzioni minime: la registrazione giornaliera può fornire un flusso di informazioni più gestibile, che può ridurre la frequenza delle notifiche e avvisare l'affaticamento.
- Efficienza in termini di costi: la registrazione giornaliera offre la flessibilità necessaria per registrare le modifiche alle risorse con una frequenza inferiore, il che può ridurre i costi legati al numero di modifiche alla configurazione registrate.

> **Note**
>
> AWS Firewall Manager dipende dalla registrazione continua per monitorare le risorse. Se si utilizza Firewall Manager, si consiglia di impostare la frequenza di registrazione su Continuo.

Interruzione della registrazione delle risorse

È possibile interrompere la registrazione AWS Config di un tipo di risorsa in qualsiasi momento. Una AWS Config volta interrotta la registrazione, una risorsa conserva le informazioni di configurazione acquisite in precedenza ed è possibile continuare ad accedere a tali informazioni.

Risorse non registrate

Se una risorsa non viene registrata, AWS Config acquisisce solo la creazione e l'eliminazione di quella risorsa e nessun altro dettaglio, senza alcun costo per l'utente. Quando una risorsa non registrata viene creata o eliminata, AWS Config invia una notifica e visualizza l'evento nella pagina dei dettagli della risorsa. La pagina dei dettagli di una risorsa non registrata contiene valori nulli per la maggior parte dei dettagli di configurazione e non fornisce informazioni sulle relazioni e sulle modifiche alla configurazione.

> **Note**
>
> I tipi di risorse `AWS::IAM::User`, `AWS::IAM::Policy`, `AWS::IAM::Group`, `AWS::IAM::Role` acquisiscono gli stati di creazione (`ResourceNotRecorded`) ed eliminazione (`ResourceDeletedNotRecorded`) solo se la risorsa è, o è stata in precedenza, selezionata come risorsa da registrare nel registratore di configurazione.

> **Note**
>
> Gli elementi di configurazione (CI) per `ResourceNotRecorded` e `ResourceDeletedNotRecorded` non seguono il tempo di registrazione tipico per i tipi di risorse. Questi tipi di risorse vengono registrati solo durante il processo di baseline periodico per il registratore di configurazione, che avviene a una cadenza meno frequente rispetto agli altri tipi di risorse.

Le informazioni sulle relazioni che AWS Config forniscono le risorse registrate non sono limitate a causa della mancanza di dati per le risorse non registrate. Se una risorsa registrata è in relazione con una risorsa non registrata, tale relazione è indicata nella pagina dei dettagli della risorsa registrata.

AWS Config Regole e tipi di risorse globali

I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) possono essere registrati solo nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse IAM globali non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta Recording AWS Resources | Global Resources.

Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.

Le migliori pratiche per la segnalazione della conformità sulle risorse globali integrate prima di febbraio 2022

Per evitare valutazioni non necessarie, dovresti distribuire AWS Config regole e pacchetti di conformità che includano queste risorse globali solo in una delle regioni supportate. Per un elenco

delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale. Ciò vale per AWS Config le regole, AWS Config le regole organizzative e anche le regole create da altri AWS servizi, come AWS Security Hub e AWS Control Tower.

Se non hai abilitato la registrazione dei tipi di risorse globali integrati prima di febbraio 2022, consigliamo di non abilitare le seguenti regole periodiche per evitare valutazioni inutili:

- access-keys-rotated
- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- mfa-enabled-for-iam-console-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

Le migliori pratiche per la segnalazione della conformità sulle risorse globali introdotte dopo febbraio 2022

I tipi di risorse globali inseriti in fase di AWS Config registrazione dopo febbraio 2022 verranno registrati solo nella regione di origine del servizio per la partizione commerciale e AWS GovCloud (Stati Uniti occidentali) per la partizione. AWS GovCloud (US) È necessario distribuire AWS Config regole e pacchetti di conformità che includano queste risorse globali solo nella regione di origine del tipo di risorsa. Per ulteriori informazioni, consulta Home Regions for Global Resource Types.

Registrazione delle configurazioni per le risorse di terze parti

Registra le configurazioni per risorse di terze parti o tipi di risorse personalizzate come server locali, strumenti di monitoraggio SAAS e sistemi di controllo delle versioni (simili). GitHub È possibile pubblicare i dati di configurazione di risorse di terze parti AWS Config e visualizzare e monitorare l'inventario delle risorse e la cronologia delle configurazioni utilizzando AWS Config console e API. Ora puoi utilizzarle AWS Config per gestire tutte le tue risorse e valutare la configurazione delle

risorse per verificarne la conformità rispetto alle migliori pratiche utilizzando AWS Config le regole. Puoi anche creare AWS Config regole o pacchetti di conformità per valutare queste risorse di terze parti rispetto alle migliori pratiche, alle politiche interne e alle politiche normative.

> **Note**
>
> Se la configurazione è stata configurata AWS Config per registrare tutti i tipi di risorse, le risorse di terze parti gestite (create, aggiornate o eliminate) tramite esse AWS CloudFormation vengono automaticamente registrate AWS Config come elementi di configurazione.

Prerequisito: le risorse di terze parti o il tipo di risorsa personalizzato devono essere registrati utilizzando. AWS CloudFormation

Argomenti

- Fase 1: Configurare l'ambiente di sviluppo
- Fase 2: Modellare la risorsa
- Passaggio 3: Generare gli artefatti
- Passaggio 4: Registrare la risorsa
- Passaggio 5: Pubblicare la configurazione della risorsa
- Registra ed elimina uno stato di configurazione per risorse di terze parti utilizzando AWS CLI
- Gestione di uno stato di configurazione per il tipo di risorsa di terze parti utilizzando le API

Fase 1: Configurare l'ambiente di sviluppo

Installa e configura AWS CloudFormation AWS CLI. Ti AWS CLI consente di modellare e registrare le tue risorse personalizzate. Per ulteriori informazioni, consulta Risorse personalizzate e Cos'è l'interfaccia a riga di CloudFormation comando? .

Fase 2: Modellare la risorsa

Crea uno schema di provider di risorse conforme e convalida la configurazione del tipo di risorsa.

1. Utilizzare il comando `init` per creare il progetto del provider di risorse e generare i file necessari.

```
$ cfn init
Initializing new project
```

2. Il comando `init` avvia una procedura guidata che illustra l'impostazione del progetto, inclusa la specificazione del nome della risorsa. Per questa procedura dettagliata, specificare `MyCustomNamespace::Testing::WordPress`.

```
Enter resource type identifier (Organization::Service::Resource):
 MyCustomNamespace::Testing::WordPress
```

3. Immettere il nome di un pacchetto per la risorsa.

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):
 com.custom.testing.wordpress
Initialized a new project in /workplace/user/custom-testing-wordpress
```

> **Note**
>
> Per assicurarti che tutte le dipendenze del progetto vengano risolte correttamente, puoi importare il progetto generato nel tuo IDE con supporto Maven.
> Se ad esempio utilizzi IntelliJ IDEA, è necessario eseguire le operazioni seguenti:
>
> - Dal menu File, seleziona Nuovo, quindi Progetto da origini esistenti.
> - Passa alla directory del progetto.
> - Nella finestra di dialogo Importa progetto, scegli Importa progetto da modello esterno, quindi scegli Maven.
> - Seleziona Avanti e accetta le impostazioni predefinite per completare l'importazione del progetto.

4. Aprire il file `mycustomnamespace-testing-wordpress.json` che contiene lo schema per la risorsa. Copiare e incollare lo schema seguente in `mycustomnamespace-testing-wordpress.json`.

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
```

```
    "Name": {
      "description": "A name associated with the website.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",
      "minLength": 1, "maxLength": 219
    },
    "SubnetId": {
      "description": "A subnet in which to host the website.",
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",
      "type": "string"
    },
    "InstanceId": {
      "description": "The ID of the instance that backs the WordPress site.",
      "type": "string"
    },
    "PublicIp": {
      "description": "The public IP for the WordPress site.",
      "type": "string"
    }
  },
  "required": [ "Name", "SubnetId" ],
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "additionalProperties": false
}
```

5. Convalidare lo schema.

```
$ cfn validate
```

6. Aggiornare i file generati automaticamente nel pacchetto del provider di risorse per visualizzare gli aggiornamenti dello schema del provider di risorse. All'avvio del progetto del fornitore di risorse, AWS CLI genera file e codice di supporto per il fornitore di risorse. Rigenerare il codice per visualizzare lo schema aggiornato.

```
$ cfn generate
```

> **Note**
>
> Se utilizzi Maven, come parte del processo di compilazione, il comando `generate` viene eseguito automaticamente prima della compilazione del codice. Quindi le modifiche saranno sempre sincronizzate con il codice generato.

> Tieni presente che la CloudFormation CLI deve trovarsi in una posizione che MAVEN/il sistema può trovare. Per ulteriori informazioni, consulta Configurazione dell'ambiente per lo sviluppo di estensioni.

Per ulteriori informazioni sulla procedura completa, consulta Modellazione del provider di risorse per l'utilizzo in AWS CloudFormation.

Passaggio 3: Generare gli artefatti

Esegui il comando seguente per generare artefatti per `cfn submit`.

```
$ mvn package
```

Passaggio 4: Registrare la risorsa

AWS Config non richiede che i gestori dei provider di risorse eseguano il monitoraggio della configurazione della risorsa. Esegui il comando seguente per registrare la risorsa.

```
$ cfn submit
```

Per ulteriori informazioni, vedere Registrazione dei provider di risorse per l'uso nei modelli. AWS CloudFormation

Passaggio 5: Pubblicare la configurazione della risorsa

Determina la configurazione per MyCustomNamespace: :Testing::. WordPress

```
{
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
  "PublicIp": "my-wordpress-site.com"
}
```

Determina l'id della versione dello schema da AWS CloudFormation `DescribeType`.

AWS Config Verifica se questa configurazione delle risorse è accettata. Per valutare la conformità è possibile scrivere AWS Config regole utilizzando questa risorsa. Per ulteriori informazioni, consulta Registrare ed eliminare uno stato di configurazione per risorse di terze parti tramite AWS CLI.

Facoltativo: per automatizzare la registrazione della configurazione, implementa i collettori di configurazione periodici o basati su modifiche.

Registra ed elimina uno stato di configurazione per risorse di terze parti utilizzando AWS CLI

AWS CLI È uno strumento unificato per gestire i tuoi AWS servizi. Con un solo strumento da scaricare e configurare, puoi controllare più AWS servizi dalla riga di comando e utilizzare script per automatizzarli. Per ulteriori informazioni sugli strumenti AWS CLI e per istruzioni sull'installazione degli AWS CLI strumenti, vedere quanto segue nella Guida per l'AWS Command Line Interface utente.

- AWS Command Line Interface Guida per l'utente
- Come configurare la AWS Command Line Interface

Se necessario, accedi `aws configure` per configurare l'utilizzo AWS CLI di una AWS regione in cui siano disponibili AWS Config gli aggregatori.

Argomenti

- Registrare un elemento di configurazione
- Lettura dell'elemento di configurazione tramite le API di AWS Config
- Eliminare la risorsa di terze parti

Registrare un elemento di configurazione

Registra un elemento di configurazione per una risorsa di terze parti o un tipo di risorsa personalizzata utilizzando la procedura seguente:

Assicurati di registrare il tipo di risorsa `MyCustomNamespace::Testing::WordPress` con lo schema corrispondente.

1. Apri un prompt dei comandi o una finestra del terminale.
2. Immetti il comando seguente:

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
```

```
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

> **Note**
>
> Come definito nello schema dei tipi, `writeOnlyProperties` verrà rimosso dalla configurazione prima di essere registrato da AWS Config. Ciò significa che questi valori non sono presenti quando la configurazione viene ottenuta tramite API di lettura. Per ulteriori informazioni su `writeOnlyProperties`, consulta Schema del tipo di risorsa.

Lettura dell'elemento di configurazione tramite le API di AWS Config

1. Apri un prompt dei comandi o una finestra del terminale.
2. Immetti il comando seguente:

```
aws configservice list-discovered-resources --resource-type
 MyCustomNamespace::Testing::WordPress
```

3. Premere Invio.

   Verrà visualizzato un output simile al seguente:

```
{
    "resourceIdentifiers": [
        {
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001"
        }
    ]
}
```

4. Immetti il comando seguente:

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":
 "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. Premere Invio.

   Verrà visualizzato un output simile al seguente:

```
{
    "unprocessedResourceKeys": [],
    "baseConfigurationItems": [
        {
            "configurationItemCaptureTime": 1569605832.673,
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001",
            "configurationStateId": "1569605832673",
            "awsRegion": "us-west-2",
            "version": "1.3",
            "supplementaryConfiguration": {},
            "configuration": "{\"Id\":\"resource-001\",\"Name\":\"My example custom
 resource.\",\"PublicAccess\":false}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "AccountId"
        }
    ]
}
```

Eliminare la risorsa di terze parti

Puoi registrare lo stato di configurazione di una risorsa di terze parti o di un tipo di risorsa personalizzato che intendi eliminare.

- Immetti il comando seguente:

```
aws configservice delete-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-002
```

  In caso di esito positivo, il comando viene eseguito senza ulteriore output.

Gestione di uno stato di configurazione per il tipo di risorsa di terze parti utilizzando le API

Puoi gestire uno stato di configurazione per risorse di terze parti o un tipo di risorsa personalizzato utilizzando le PutResourceAPI Config e Config. DeleteResource Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di .

- PutResourceConfig
- DeleteResourceConfig

Registrazione della configurazione del software per le istanze gestite

Puoi utilizzarlo AWS Config per registrare le modifiche all'inventario software sulle istanze Amazon EC2 e sui server locali. In questo modo puoi visualizzare la cronologia delle modifiche alla configurazione del software. Ad esempio, quando un nuovo aggiornamento di Windows viene installato su un'istanza Windows gestita, AWS Config registra le modifiche e quindi le invia al canale di distribuzione, in modo da ricevere una notifica della modifica. Con AWS Config, puoi vedere la cronologia di quando sono stati installati gli aggiornamenti di Windows per l'istanza gestita e come sono cambiati nel tempo.

Per registrare le modifiche di configurazione del software devi completare i seguenti passaggi:

- Attivare la registrazione per il tipo di risorsa inventario software dell'istanza gestita in AWS Config.
- Configurare i server EC2 e locali come istanze gestite in AWS Systems Manager. Un'istanza gestita è un computer configurato per l'uso con Systems Manager.
- Avviare la raccolta della inventario software dalle istanze gestite usando la funzionalità Inventario di Systems Manager.

> **Note**
>
> Systems Manager ora supporta la creazione di elementi di configurazione per istanze non gestite
> L'elemento di configurazione per le istanze non gestite avrà una configurazione supplementare con `Key: “InstanceStatus”` e `Value: “Unmanaged”`.

Gli elementi di configurazione per le istanze non gestite non riceveranno aggiornamenti aggiuntivi
Per ricevere ulteriori aggiornamenti, l'elemento di configurazione deve essere un'istanza gestita.

Puoi anche utilizzare AWS Config le regole per monitorare le modifiche alla configurazione del software e ricevere una notifica se le modifiche sono conformi o non conformi alle tue regole. Ad esempio, se crei una regola che verifica se le istanze gestite hanno un'applicazione specifica e su un'istanza non è installata tale applicazione, AWS Config contrassegna tale istanza come non conforme alla regola. Per un elenco delle regole gestite, consulta. AWS Config Elenco di regole AWS Config gestite

Per abilitare la registrazione delle modifiche alla configurazione del software in AWS Config:

1. Attivare la registrazione per tutti i tipi di risorse supportati o in modo selettivo per il tipo di risorsa inventario software dell'istanza gestita in AWS Config. Per ulteriori informazioni, consulta AWS Risorse per la registrazione.
2. Avvia un'istanza Amazon EC2 con un profilo di istanza per Systems Manager che include la policy gestita di AmazonSSM ManagedInstanceCore. Questa policy gestita AWS consente a un'istanza di usare la funzionalità core del servizio Systems Manager.

   Per informazioni su altre policy che puoi aggiungere al profilo dell'istanza per Systems Manager, consulta Creazione di un profilo dell'istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager .

   Important

   L'Agente SSM è un software Amazon che deve essere installato in un'istanza gestita per comunicare con Systems Manager nel cloud. Se l'istanza EC2 è stata creata da un'AMI per uno dei seguenti sistemi operativi, l'agente è preinstallato:

   - AMI Windows Server 2003-2012 R2 pubblicate a novembre 2016 o versioni successive
   - Windows Server 2016 e 2019
   - Amazon Linux
   - Amazon Linux 2

- Server Ubuntu 16.04
- Server Ubuntu 18.04

Nelle istanze EC2 che non sono state create da un'AMI con l'agente preinstallato, è necessario installare manualmente l'agente. Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente di AWS Systems Manager :

- Installazione e configurazione dell'Agente SSM sulle istanze EC2 per Windows Server
- Installazione e configurazione dell'Agente SSM su istanze EC2 per Linux

3. Avvia la raccolta dell'inventario come descritto in Configurazione della raccolta dell'inventario nella Guida per l'utente di AWS Systems Manager . Le procedure sono le stesse per le istanze Linux e Windows.

   AWS Config può registrare le modifiche alla configurazione per i seguenti tipi di inventario:

   - Applicazioni: un elenco di applicazioni delle istanze gestite, ad esempio il software antivirus.
   - AWS componenti: un elenco di AWS componenti per le istanze gestite, ad esempio gli SDK AWS CLI e.
   - Informazioni sull'istanza: informazioni sull'istanza come nome e versione del sistema operativo, dominio e stato del firewall.
   - Configurazione di rete: informazioni di configurazione come indirizzo IP, gateway e subnet mask.
   - Aggiornamenti di Windows: un elenco di aggiornamenti di Windows per le istanze gestite (solo per istanze Windows).

   > **Note**
   >
   > AWS Config al momento non supporta la registrazione del tipo di inventario personalizzato.

La raccolta dell'inventario è una delle numerose funzionalità di Systems Manager, raggruppate nelle categorie Gestione delle operazioni, Operazioni e modifiche, Istanze e nodi e Risorse condivise.

Per ulteriori informazioni, consulta la pagina Cos'è Systems Manager? e Funzionalità di Systems Manager nella Guida per l'utente di AWS Systems Manager .

Visualizzazione delle configurazioni e della cronologia delle risorse di

AWS Config È possibile visualizzare tutte le risorse registrate nel proprio account, le modifiche alla configurazione apportate a una risorsa in un periodo di tempo specificato e le relazioni della risorsa selezionata con tutte le risorse correlate. È inoltre possibile visualizzare le modifiche dello stato di conformità delle risorse, valutate mediante Regole di AWS Config visualizzazione in una sequenza temporale.

Argomenti

- Ricerca di risorse scoperte da AWS Config
- Visualizzazione delle informazioni sulla conformità e dei risultati della valutazione
- Visualizzazione della cronologia di configurazione e conformità

Ricerca di risorse scoperte da AWS Config

Puoi utilizzare la AWS Config console e l' AWS Config API per cercare le risorse che sono AWS Config state inventariate o scoperte, comprese le risorse eliminate e le risorse che AWS Config non sono attualmente in fase di registrazione. AWS CLI AWS Config rileva solo i tipi di risorse supportati. Per ulteriori informazioni, consulta Tipi di risorsa supportati.

Ricerca tra le risorse (Console)

Puoi utilizzare i tipi di risorse o le informazioni sui tag per cercare tra risorse nella console AWS Config .

Per cercare risorse (Console)

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Nella pagina Inventario risorse, specifica le opzioni di ricerca per le risorse desideri cercare:
    - Categoria di risorse: scegli tutte le categorie di risorse o restringi i risultati alle sole AWS risorse.

- Tipo di risorsa: scegli tutti i tipi di risorse o seleziona le risorse in base alle quali filtrare.
- Conformità: scegli di filtrare in base a qualsiasi stato di conformità, conforme o non conforme.

3. AWS Config elenca le risorse che corrispondono alle opzioni di ricerca. Puoi visualizzare le seguenti informazioni sulle risorse:

   - Identificatore risorsa: l'identificatore della risorsa potrebbe essere un ID di risorsa o un nome di risorsa, se applicabile. Selezionare il collegamento dell'identificatore della risorsa per visualizzare la pagina di dettaglio della risorsa.
   - Tipo di risorsa: viene elencato il tipo di risorsa.
   - Conformità: lo stato della risorsa che è AWS Config stata valutata in base alla tua regola.

     Per ulteriori informazioni, consulta Visualizzazione della cronologia di configurazione e conformità.

Ricerca tra le risorse (AWS CLI)

È possibile utilizzare il AWS CLI per elencare le risorse che sono AWS Config state scoperte.

Per cercare tra le risorse (AWS CLI)

Utilizza il comando AWS Config service **`list-discovered-resources`**:

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
        {
            "resourceIdentifiers": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-nnnnnnnn"
                }
            ]
        }
```

Per visualizzare i dettagli di configurazione di una risorsa elencata nella risposta, utilizzare il comando `get-resource-config-history` e specificare il tipo e l'ID della risorsa. Per un esempio di questo comando e della risposta di AWS Config, vediVisualizzazione della cronologia della configurazione.

Ricerca tra le risorse (API)

Si specifica un tipo di risorsa e si AWS Config restituisce un elenco di identificatori di risorsa per le risorse di quel tipo. Per ulteriori informazioni, consulta ResourceIdentifierl'AWS Config API Reference.

Per cercare risorse (API)

Usa l'azione ListDiscoveredResources.

Per ottenere i dettagli di configurazione di una risorsa elencata nella risposta, utilizza l'GetResourceConfigHistoryazione e specifica il tipo e l'ID della risorsa.

Visualizzazione delle informazioni sulla conformità e dei risultati della valutazione

> **Important**
>
> Per creare report accurati sullo stato di conformità, devi registrare il tipo di risorsa `AWS::Config::ResourceCompliance`. Per ulteriori informazioni, consulta Recoding Resources AWS.

Puoi utilizzare la AWS Config console o gli AWS SDK per visualizzare le informazioni sulla conformità e i risultati della valutazione delle tue regole e risorse.

Indice

- Visualizzazione della conformità (console)
- Visualizzazione della conformità (AWS SDK)

Visualizzazione della conformità (console)

Per visualizzare la conformità (console)

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Nel AWS Management Console menu, verifica che il selettore di regione sia impostato su una regione che supporta AWS Config le regole. Per un elenco delle regioni supportate, consultaRegioni ed endpoint di AWS Config nei Riferimenti generali di Amazon Web Services.

3. Nel riquadro di spostamento seleziona Resources (Risorse). Nella pagina Inventario risorse, puoi filtrare per categoria di risorse, tipo di risorsa e stato di conformità. Se necessario, scegli Includi risorse eliminate. La tabella visualizza l'identificatore di risorse per il tipo di risorsa e lo stato di conformità della risorsa. L'identificatore della risorsa potrebbe essere un ID di risorsa o un nome di risorsa.
4. Scegli una risorsa dalla colonna dell'identificatore della risorsa.
5. Seleziona il pulsante Cronologia della risorsa. È possibile filtrare per eventi di configurazione, eventi di conformità o CloudTrail eventi.

> **Note**
>
> In alternativa, nella pagina Inventario risorse, puoi scegliere direttamente il nome della risorsa. Per accedere alla cronologia delle risorse dalla pagina dei dettagli della risorsa, seleziona il pulsante Cronologia della risorsa.

Per visualizzare la conformità delle tue risorse puoi anche controllare la pagina Resource inventory (Inventario risorse). Per ulteriori informazioni, consulta Ricerca di risorse scoperte da AWS Config.

Visualizzazione della conformità (AWS SDK)

Per ottenere informazioni sulla conformità delle tue AWS Config regole

I seguenti esempi di codice mostrano come utilizzare`DescribeComplianceByConfigRule`.

CLI

AWS CLI

Per ottenere informazioni sulla conformità per le regole di AWS Config

Il comando seguente restituisce informazioni sulla conformità per ogni regola di AWS Config violata da una o più risorse: AWS

```
aws configservice describe-compliance-by-config-rule --compliance-types
 NON_COMPLIANT
```

Nell'output, il valore di ogni `CappedCount` attributo indica quante risorse non sono conformi alla regola correlata. Ad esempio, l'output seguente indica che 3 risorse non sono conformi alla regola denominata`InstanceTypesAreT2micro`.

Output:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Per i dettagli sull'API, consulta DescribeComplianceByConfigRule AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio recupera i dettagli di conformità per la regola ebs-optimized-instance, per la quale non esistono risultati di valutazione correnti per la regola, quindi restituisce INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Output:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Esempio 2: questo esempio restituisce il numero di risorse non conformi per la regola ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Per i DescribeComplianceByConfigRuledettagli AWS Tools for PowerShell sull'API, vedere in Cmdlet Reference.

Per ottenere informazioni sulla conformità delle tue risorse AWS

I seguenti esempi di codice mostrano come utilizzare`DescribeComplianceByResource`.

CLI

AWS CLI

Per ottenere informazioni sulla conformità delle tue AWS risorse

Il comando seguente restituisce informazioni sulla conformità per ogni istanza EC2 registrata da AWS Config e che viola una o più regole:

```
aws configservice describe-compliance-by-resource --resource-type
 AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

Nell'output, il valore di ogni `CappedCount` attributo indica quante regole la risorsa viola. Ad esempio, l'output seguente indica che l'istanza `i-1a2b3c4d` viola 2 regole.

Output:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- Per i dettagli sull'API, consulta DescribeComplianceByResource AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio verifica il tipo di **`AWS::SSM::ManagedInstanceInventory`** risorsa per il tipo di conformità «COMPLIANT».

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Output:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Per i dettagli sull'API, vedere DescribeComplianceByResourcein AWS Tools for PowerShell Cmdlet Reference.

Per ottenere il riepilogo della conformità delle tue regole AWS Config

I seguenti esempi di codice mostrano come utilizzare`GetComplianceSummaryByConfigRule`.

CLI

AWS CLI

Per ottenere il riepilogo della conformità per le tue regole di AWS Config

Il comando seguente restituisce il numero di regole conformi e il numero di regole non conformi:

```
aws configservice get-compliance-summary-by-config-rule
```

Nell'output, il valore di ogni `CappedCount` attributo indica quante regole sono conformi o non conformi.

Output:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
```

```
}
```

- Per i dettagli sull'API, consulta Command Reference. GetComplianceSummaryByConfigRuleAWS CLI

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio restituisce il numero di regole di Config non conformi.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Per i dettagli sull'API, vedere GetComplianceSummaryByConfigRulein Cmdlet Reference.AWS Tools for PowerShell

Per ottenere il riepilogo della conformità delle tue risorse AWS

I seguenti esempi di codice mostrano come utilizzare`GetComplianceSummaryByResourceType`.

CLI

AWS CLI

Per ottenere il riepilogo della conformità per tutti i tipi di risorse

Il comando seguente restituisce il numero di AWS risorse non conformi e il numero di risorse conformi:

```
aws configservice get-compliance-summary-by-resource-type
```

Nell'output, il valore di ogni `CappedCount` attributo indica quante risorse sono conformi o non conformi.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

Per ottenere il riepilogo della conformità per un tipo di risorsa specifico

Il comando seguente restituisce il numero di istanze EC2 non conformi e il numero di istanze conformi:

```
aws configservice get-compliance-summary-by-resource-type --resource-types
 AWS::EC2::Instance
```

Nell'output, il valore di ogni `CappedCount` attributo indica quante risorse sono conformi o non conformi.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
```

```
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- Per i dettagli sull'API, consulta Command Reference. GetComplianceSummaryByResourceTypeAWS CLI

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio restituisce il numero di risorse conformi o non conformi e converte l'output in json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Per i dettagli sull'API, vedere in Cmdlet Reference. GetComplianceSummaryByResourceTypeAWS Tools for PowerShell

Per ottenere i risultati della valutazione per una regola AWS Config

I seguenti esempi di codice mostrano come utilizzare`GetComplianceDetailsByConfigRule`.

CLI

AWS CLI

Per ottenere i risultati della valutazione per una regola di AWS Config

Il comando seguente restituisce i risultati della valutazione per tutte le risorse che non sono conformi a una regola AWS Config denominata: `InstanceTypesAreT2micro`

```
aws configservice get-compliance-details-by-config-rule --config-rule-name
 InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
```

```
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Per i dettagli sull'API, consulta GetComplianceDetailsByConfigRule AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio ottiene i risultati della valutazione per la regola access-keys-rotated e restituisce l'output raggruppato per tipo di conformità

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Output:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Esempio 2: questo esempio richiede i dettagli di conformità per la regola per le risorse COMPLIANT. access-keys-rotated

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Output:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Per i dettagli sull'API, vedere GetComplianceDetailsByConfigRulein AWS Tools for PowerShell Cmdlet Reference.

Per ottenere i risultati della valutazione di una risorsa AWS

I seguenti esempi di codice mostrano come usare`GetComplianceDetailsByResource`.

CLI

AWS CLI

Per ottenere i risultati della valutazione di una AWS risorsa

Il comando seguente restituisce i risultati della valutazione per ogni regola a cui l'istanza EC2 `i-1a2b3c4d` non è conforme:

```
aws configservice get-compliance-details-by-resource --resource-type
 AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
```

```
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Per i dettagli sull'API, consulta GetComplianceDetailsByResource AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: Questo esempio di risultati di valutazione per la risorsa data.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Output:

```
Annotation                :
ComplianceType            : COMPLIANT
ConfigRuleInvokedTime     : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime        : 8/25/2019 11:34:56 PM
```

```
ResultToken                 :
```

- Per i dettagli sull'API, vedere GetComplianceDetailsByResourcein AWS Tools for PowerShell Cmdlet Reference.

Visualizzazione della cronologia di configurazione e conformità

> **Important**
>
> Per creare report accurati sullo stato di conformità, devi registrare il tipo di risorsa `AWS::Config::ResourceCompliance`. Per ulteriori informazioni, consulta Recoding Resources. AWS

È possibile visualizzare la configurazione, le relazioni e il numero di modifiche apportate a una risorsa nella AWS Config console. È possibile visualizzare la cronologia di configurazione di una risorsa utilizzando AWS CLI.

Visualizzazione dei dettagli della configurazione (Console)

Visualizzazione dei dettagli di configurazione tramite la console

Quando cerchi risorse nella pagina Inventario risorse, scegli il nome della risorsa o l'ID nella colonna dell'identificatore di risorse per visualizzare la pagina dei dettagli della risorsa. La pagina dei dettagli fornisce informazioni sulla configurazione, sulle relazioni e sul numero di modifiche apportate a tale risorsa.

Per accedere alla cronologia delle risorse dalla pagina dei dettagli della risorsa, seleziona il pulsante Cronologia della risorsa. La cronologia della risorsa acquisisce le modifiche come `ConfigurationItems` in un periodo di tempo per una risorsa specifica. È possibile filtrare per eventi di configurazione, eventi di conformità o CloudTrail eventi.

Visualizzazione dei dettagli della configurazione (AWS CLI)

Visualizzazione dei dettagli di configurazione utilizzando il AWS CLI

Gli elementi di configurazione AWS Config registrati vengono consegnati al canale di distribuzione specificato su richiesta come istantanea di configurazione e come flusso di configurazione. È possibile utilizzare il AWS CLI per visualizzare la cronologia degli elementi di configurazione per ogni risorsa.

Visualizzazione della cronologia della configurazione

Digitare il comando `get-resource-config-history` e specificare il tipo di risorsa e l'ID della risorsa, ad esempio:

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
```

```
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```

Per una spiegazione dettagliata dei campi della risposta, consulta Components of a Configuration Item e Tipi di risorsa supportati.

Esempio di cronologia della configurazione Amazon EBS da AWS Config

AWS Config genera un set di file che rappresentano ciascuno un tipo di risorsa ed elenca tutte le modifiche alla configurazione per le risorse di quel AWS Config tipo in fase di registrazione. AWS Config esporta questa cronologia di configurazione incentrata sulle risorse come oggetto nel bucket Amazon S3 che hai specificato al momento dell'attivazione. AWS Config Il file della cronologia della configurazione per ogni tipo di risorsa contiene le modifiche che sono state rilevate per le risorse di quel tipo a partire dall'ultimo file di cronologia che è stato distribuito. I file della cronologia sono generalmente distribuiti ogni sei ore.

Di seguito è riportato un esempio del contenuto dell'oggetto Amazon S3 che descrive la cronologia di configurazione di tutti i volumi Amazon Elastic Block Store nella regione corrente per la tua. Account AWS I volumi di questo account includono `vol-ce676ccc` e `vol-cia007c`. Il volume `vol-ce676ccc` ha subito due modifiche della configurazione a partire dal file della cronologia precedentemente distribuito mentre il volume `vol-cia007c` ha subito una modifica.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
```

```
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
```

```
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-ad229edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04w292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
```

```
                    "device": "/dev/sdf",
                    "state": "attached",
                    "attachTime": "2014-03-07T23:46:28.0000+0000",
                    "deleteOnTermination": false
                }
            ],
            "tags": [
                {
                    "tagName": "environment",
                    "tagValue": "PROD"
                },
                {
                    "tagName": "name",
                    "tagValue": "DataVolume1"
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "vol-cia007c",
        "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
        "accountId": "12345678910",
        "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
        "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
            "c376e30d-71a2-4694-89b7-a5a67u292281"
        ],
        "availibilityZone": "us-west-2b",
        "resourceType": "AWS::EC2::Volume",
        "resourceCreationTime": "2014-02-27T20:43:53.885Z",
        "tags": {},
        "relationships": [
            {
                "resourceId": "i-344e563d",
                "resourceType": "AWS::EC2::Instance",
                "name": "Attached to Instance"
            }
        ],
        "configuration": {
            "volumeId": "vol-cia007c",
```

```
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T20:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-cia007c",
                        "instanceId": "i-344e563d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
}
```

Visualizzazione della cronologia di conformità per le risorse

AWS Config supporta la memorizzazione delle modifiche dello stato di conformità delle risorse secondo la valutazione di. Regole di AWS Config La cronologia di conformità delle risorse viene presentata sotto forma di sequenza temporale. La sequenza temporale acquisisce le modifiche come `ConfigurationItems` in un periodo di tempo per una risorsa specifica. Per informazioni sui contenuti di`ConfigurationItem`, consulta ConfigurationItemI' AWS Config API Reference.

Puoi scegliere di registrare o meno tutti i tipi di risorse in AWS Config. Se hai scelto di registrare tutti i tipi di risorse, inizia AWS Config automaticamente a registrare la cronologia della conformità delle risorse valutata da. Regole di AWS Config Per impostazione predefinita, AWS Config

registra le modifiche alla configurazione per tutte le risorse supportate. Puoi selezionare anche solo il tipo di risorsa specifico relativo alla cronologia di conformità delle risorse: `AWS::Config::ResourceCompliance`. Per ulteriori informazioni, vedere Selezione dei AWS Config record di risorse.

Visualizzazione della cronologia delle risorse utilizzando le risorse

Accedi alla cronologia delle risorse selezionando una risorsa specifica dalla pagina Inventario risorse.

1. Scegli le Risorse dal pannello di navigazione a sinistra.
2. Nella pagina Inventario risorse, puoi filtrare per categoria di risorse, tipo di risorsa e stato di conformità. Se necessario, scegli Includi risorse eliminate.

   La tabella visualizza l'identificatore di risorse per il tipo di risorsa e lo stato di conformità della risorsa. L'identificatore della risorsa potrebbe essere un ID di risorsa o un nome di risorsa.
3. Scegli una risorsa dalla colonna dell'identificatore della risorsa.
4. Seleziona il pulsante Cronologia della risorsa. È possibile filtrare per eventi di configurazione, eventi di conformità o CloudTrail eventi.

> **Note**
>
> In alternativa, nella pagina Inventario risorse, puoi scegliere direttamente il nome della risorsa. Per accedere alla cronologia delle risorse dalla pagina dei dettagli della risorsa, seleziona il pulsante Cronologia della risorsa.

Visualizzazione della cronologia delle risorse utilizzando le regole

Accedi alla cronologia delle risorse selezionando una regola specifica dalla pagina Regola.

1. Selezionare le Regole dal pannello di navigazione a sinistra.
2. Nella pagina Regola, scegli una regola per valutare le risorse pertinenti. Se nessuna delle regole viene visualizzata sullo schermo, aggiungere regole utilizzando il pulsante Aggiungi regola.
3. Nella pagina di dettaglio delle regole, selezionare le risorse dalla tabella delle Risorse valutate.
4. Seleziona il pulsante Cronologia della risorsa. Viene visualizzata la cronologia della risorsa.

Query sulla cronologia di conformità

Esegui una query sulla cronologia della conformità delle risorse get-resource-config-history utilizzando il tipo di risorsa`AWS::Config::ResourceCompliance`.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

Verrà visualizzato un output simile al seguente:

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
     "resourceType": "AWS::S3::Bucket",
     "resourceId": "configrules-bucket",
     "relationshipName": "Is associated with "
    }
   ]
   "tags": {},
   "resourceType": "AWS::Config::ResourceCompliance",
   "resourceId": "AWS::S3::Bucket/configrules-bucket",
   "ConfigurationStateId": "1539799966921",
   "relatedEvents": [];
   "awsRegion": "us-west-2",
   "version": "1.3",
   "configurationItemMD5Hash": "",
   "supplementaryConfiguration": {},
   "configuration": "{\"complianceType\":\"COMPLIANT\",\"targetResourceId\":
\"configrules-bucket\",\"targetResourceType\":\"AWS::S3::Bucket\",\configRuleList"\":
[{\"configRuleArn\":\"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-w1gogw
\",\"configRuleId\":\"config-rule-w1gogw\",\"configRuleName\":\"s3-bucket-logging-
enabled\",\"complianceType\":\"COMPLIANT\"}]}",

   "configurationItemStatus": "ResourceDiscovered",
   "accountId": "AccountID"
  }
 ]
}
```

Tagging delle risorse AWS Config

Un tag è un'etichetta che assegni a una risorsa AWS. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili. I tag semplificano la gestione, la ricerca e il filtro delle risorse.

I tag consentono di categorizzare le tue risorse AWS in modi diversi, ad esempio, per scopo, proprietario o ambiente. Questa funzionalità è molto utile quando hai tante risorse dello stesso tipo: puoi rapidamente individuare una risorsa specifica in base ai tag assegnati. Puoi assegnare uno o più tag alleAWS risorse. A ogni tag è associato un valore.

Ti consigliamo di creare un set di chiavi di tag in grado di soddisfare i requisiti di ciascun tipo di risorsa. Tramite un set di chiavi di tag coerente la gestioneAWS delle risorse risulta notevolmente semplificata. Puoi cercare e filtrare le risorse in base ai tag aggiunti.

I tag vengono interpretati rigorosamente come una stringa di caratteri e non vengono assegnati automaticamente alle risorse. Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Puoi impostare il valore di un tag su una stringa vuota, ma non su null. Se aggiungi un tag con la stessa chiave di un tag esistente a una risorsa specifica, il nuovo valore sovrascrive quello precedente. Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa.

Puoi lavorare con i tag utilizzando AWS Command Line Interface (AWS CLI) e il riferimento delle API di AWS Config.

Limitazioni relative al tagging

Ai tag si applicano le seguenti limitazioni di base.

Limitazione	Descrizione
Numero massimo di tag per risorsa	50
Lunghezza massima chiave	128 caratteri Unicode in UTF-8
Lunghezza massima del valore	256 caratteri Unicode in UTF-8
Limitazione dei prefissi	Non utilizzare il prefisso `aws:` nei nomi o nei valori di tag perché è riservato per essere

Limitazione	Descrizione
	utilizzato in AWS. Non è possibile modificar e né eliminare i nomi o i valori di tag con tale prefisso. I tag con questo prefisso non vengono conteggiati per il limite del numero di tag per risorsa.
Limitazioni di caratteri	I tag possono contenere solo lettere unicode, cifre, spazi vuoti o questi simboli: `_ . : / = + - @`

Gestione dei tag con le operazioni API AWS Config

I controlli di accesso basati su tag sono disponibili per tre risorse `ConfigurationAggregator`, `AggregationAuthorization` e `ConfigRule`. Utilizza le seguenti informazioni per aggiungere, aggiornare, elencare ed eliminare i tag per le risorse.

- ListTagsForResource
- TagResource
- UntagResource

> **Note**
>
> `TagResourceeUntagResource` richiedono determinate autorizzazioniAWS Identity and Access Management (IAM) per controllare l'accesso. Per ulteriori informazioni, consulta Controllo dell'accesso mediante i tag delle risorse nella Guida per l'utente IAM.

Valutazione delle risorse con regole AWS Config

AWS Config Da utilizzare per valutare le impostazioni di configurazione AWS delle risorse. A tale scopo, è necessario creare AWS Config regole che rappresentano le impostazioni di configurazione ideali. AWS Config fornisce regole personalizzabili e predefinite denominate regole gestite per aiutarti a iniziare.

Come funzionano AWS Config le regole

AWS Config monitora continuamente le modifiche alla configurazione che si verificano tra le risorse e verifica se queste modifiche non sono conformi con le condizioni nelle regole. Se una risorsa non è conforme alla regola, AWS Config contrassegna la risorsa e la regola come non conformi. Di seguito sono riportati i possibili risultati di valutazione per una regola: AWS Config

- `COMPLIANT`: la regola supera le condizioni del controllo di conformità.
- `NON_COMPLIANT`: la regola non rispetta le condizioni del controllo di conformità.
- `ERROR`: uno dei parametri richiesti/facoltativi non è valido, non è del tipo corretto o è formattato in modo errato.
- `NOT_APPLICABLE`: utilizzato per filtrare le risorse a cui non può essere applicata la logica della regola. Ad esempio, la regola alb-desync-mode-check verifica solo gli Application Load Balancer e ignora i Network Load Balancer e i Gateway Load Balancer.

Ad esempio, quando viene creato un volume EC2, è AWS Config possibile valutare il volume in base a una regola che richiede la crittografia dei volumi. Se il volume non è crittografato, AWS Config contrassegna il volume e la regola come non conformi. AWS Config puoi anche controllare tutte le tue risorse per verificare i requisiti a livello di account. Ad esempio, AWS Config può verificare se il numero di volumi EC2 in un account rientra nel totale desiderato o se un account lo utilizza AWS CloudTrail per la registrazione.

Regole collegate ai servizi

Le regole collegate ai servizi sono un tipo unico di regola gestita che supporta altri AWS servizi per creare AWS Config regole nell'account. Queste regole sono predefinite e includono tutte le autorizzazioni necessarie per chiamare altri AWS servizi per tuo conto. Queste regole sono simili agli standard consigliati da un AWS servizio Account AWS per la verifica della conformità. Per ulteriori informazioni, consulta Regole collegate ai servizi AWS Config.

Regole personalizzate

Puoi anche creare regole personalizzate per valutare risorse aggiuntive che AWS Config non sono ancora state registrate. Per ulteriori informazioni, consulta AWS Config Regole personalizzate e Valutazione tipi di risorse aggiuntive.

Visualizzazione della conformità

La AWS Config console mostra lo stato di conformità delle regole e delle risorse. Puoi vedere in che modo AWS le tue risorse sono complessivamente conformi alle configurazioni desiderate e scoprire quali risorse specifiche non sono conformi. Puoi anche utilizzare la AWS CLI, l' AWS Config API e gli AWS SDK per inviare richieste al AWS Config servizio di informazioni sulla conformità.

Utilizzando AWS Config per valutare le configurazioni delle risorse, è possibile valutare la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.

Limitazioni

Per il numero massimo di AWS Config regole per ogni regione per ogni account e altri limiti di servizio, consulta Limiti del AWS Config servizio.

Considerazioni sui costi

Per informazioni dettagliate sui costi associati alla registrazione delle risorse, consulta AWS Config i prezzi.

Consiglio: interrompi la registrazione della conformità delle risorse prima di eliminare le regole

Si consiglia vivamente di interrompere la registrazione per il tipo di `AWS::Config::ResourceCompliance` risorsa prima di eliminare le regole nell'account. L'eliminazione delle regole crea elementi di configurazione (CI) `AWS::Config::ResourceCompliance` e può influire sui costi del registratore AWS Config di configurazione. Se si eliminano regole che valutano un gran numero di tipi di risorse, ciò può portare a un picco nel numero di CI registrati.

Procedura ottimale:

1. Interrompi la registrazione `AWS::Config::ResourceCompliance`
2. Eliminare una o più regole
3. Attiva la registrazione per `AWS::Config::ResourceCompliance`

Raccomandazione: aggiungi una logica per gestire la valutazione delle risorse eliminate per le regole lambda personalizzate

Quando si creano regole lambda AWS Config personalizzate, si consiglia vivamente di aggiungere la logica per gestire la valutazione delle risorse eliminate.

Quando i risultati della valutazione sono contrassegnati come `NOT_APPLICABLE`, verranno contrassegnati per l'eliminazione e ripuliti. Se NON sono contrassegnate come`NOT_APPLICABLE`, i risultati della valutazione rimarranno invariati fino all'eliminazione della regola, il che può causare un picco imprevisto nella creazione di elementi della configurazione in caso di eliminazione della regola. `AWS::Config::ResourceCompliance`

Per informazioni su come impostare regole lambda AWS Config personalizzate da restituire `NOT_APPLICABLE` per le risorse eliminate, consulta Gestione delle risorse eliminate con AWS Config regole lambda personalizzate.

Raccomandazione: fornisci le risorse previste per le regole lambda personalizzate

AWS Config Le regole Lambda personalizzate possono causare un numero elevato di chiamate di funzioni Lambda se la regola non è limitata a uno o più tipi di risorse. Per evitare un aumento dell'attività associata al tuo account, ti consigliamo vivamente di fornire risorse nell'ambito delle regole Lambda personalizzate. Se non viene selezionato alcun tipo di risorsa, la regola richiamerà la funzione Lambda per tutte le risorse dell'account.

Supporto nelle regioni

Attualmente, la funzionalità AWS Config Rule è supportata nelle seguenti AWS regioni. Per un elenco delle singole AWS Config regole supportate in quali regioni, vedi Elenco delle regole AWS Config gestite per disponibilità regionale.

Nome della regione	Regione	Endpoint	Protocollo	
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
		config-fips.us-east-2.amazonaws.com	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Stati Uniti occidentali (California settentrionale)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asia Pacifico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pacific (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia Pacifico (Giacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacifico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacifico (Osaka-Locale)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacifico (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacifico (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacifico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Centrale)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Canada occidentale (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Francoforte)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londra)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milano)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Parigi)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spagna)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zurigo)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israele (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Medio Oriente (Bahrein)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (Emirati Arabi Uniti)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Sud America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

L'implementazione AWS Config delle regole tra gli account dei membri di un' AWS organizzazione è supportata nelle seguenti regioni.

Nome della regione	Regione	Endpoint	Protocollo	
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
Stati Uniti occidentali (California settentrionale)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
Asia Pacifico (Giacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Asia Pacifico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
Asia Pacifico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacifico (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacifico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Centrale)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europa (Francoforte)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londra)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Parigi)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Europa (Stoccolma)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Sud America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Componenti di una AWS Config regola

AWS Config le regole valutano le impostazioni di configurazione AWS delle risorse. Esistono due tipi di regole: Regole gestite da AWS Config e Regole personalizzate di AWS Config .

AWS Config Le regole gestite sono regole predefinite e personalizzabili create da AWS Config. Per un elenco delle regole gestite, vedere Elenco delle regole AWS Config gestite.

AWS Config Le regole personalizzate sono regole create da zero. Esistono due modi per creare regole AWS Config personalizzate: con le funzioni Lambda (AWS Lambda Developer Guide) e con Guard (Guard GitHub Repository), un linguaggio. policy-as-code AWS Config le regole personalizzate create con AWS Lambda sono chiamate Regole Lambda AWS Config personalizzate

e le regole AWS Config personalizzate create con Guard sono chiamate Regole di policy AWS Config personalizzate.

Questa pagina illustra i metadati delle regole AWS Config gestite e le migliori pratiche su come scrivere regole AWS Config personalizzate con Python utilizzando il Rules Development Kit (RDK) e la AWS Config Rules Development Kit Library (AWS Config RDKLib).

Per una procedura dettagliata che mostra come creare regole di policy personalizzate, vedi Creazione di regole di policy AWS Config personalizzate. AWS Config Per una procedura dettagliata che mostra come creare regole AWS Config Lambda personalizzate, vedi Creazione di regole Lambda personalizzate AWS Config.

Indice

- AWS Config metadati delle regole gestite
- AWS Config struttura di regole personalizzata
  - Regole di scrittura
  - Logica della regola

AWS Config metadati delle regole gestite

AWS Config le regole gestite possono contenere i seguenti metadati mutabili:

defaultName

Il nome predefinito (defaultName) è il nome che le istanze di una regola ricevono per impostazione predefinita.

description

La descrizione (description) della regola fornisce un contesto per ciò che la regola valuta. La console AWS Config ha un limite di 256 caratteri. Come best practice, la descrizione della regola deve iniziare con "Verifica se" e deve includere una descrizione dello scenario NON_COMPLIANT. I nomi dei servizi devono essere scritti per intero iniziando con AWS o Amazon quando vengono menzionati per la prima volta nella descrizione della regola. Ad esempio, AWS CloudTrail o Amazon CloudWatch al posto CloudTrail o CloudWatch per il primo utilizzo. I nomi dei servizi possono essere abbreviati in seguito per riferimento successivo.

scope

L'ambito (scope) determina i tipi di risorsa a cui si rivolge la regola. Per un elenco di tipi di risorsa supportati, consulta Tipi di risorsa supportati.

Dettagli obbligatori InputParameter

I compulsoryInputParameter dettagli vengono utilizzati per i parametri necessari alla valutazione di una regola. Ad esempio, la regola gestita `access-keys-rotated` include `maxAccessKeyAge` come parametro obbligatorio. Se un parametro è obbligatorio, non viene contrassegnato come (opzionale). Per ogni parametro, è necessario specificare un tipo. Il tipo può essere uno tra «String», «int», «double», «CSV», «boolean» e "». StringMap

Dettagli opzionali InputParameter

I optionalInputParameter dettagli vengono utilizzati per i parametri che sono facoltativi per la valutazione di una regola. Ad esempio, la regola gestita da `elasticsearch-logs-to-cloudwatch` include `logTypes` come parametro opzionale. Per ogni parametro, è necessario specificare un tipo. Il tipo può essere uno tra «String», «int», «double», «CSV», «boolean» e "». StringMap

supportato EvaluationModes

supportedEvaluationModes determina quando le risorse verranno valutate, prima che una risorsa sia stata distribuita o dopo la distribuzione di una risorsa.

`DETECTIVE` è utilizzato per valutare le risorse che sono già state implementate. Ciò consente di valutare le impostazioni di configurazione delle risorse esistenti. `PROACTIVE` viene utilizzato per valutare le risorse prima che vengano implementate.

Ciò consente di valutare se un insieme di proprietà delle risorse, se utilizzato per definire una AWS risorsa, sarebbe CONFORME o NON_COMPLIANT, in base all'insieme di regole proattive che hai nel tuo account nella tua regione.

È possibile specificare a, o entrambi e supportedEvaluationModes . `DETECTIVE` `PROACTIVE` `DETECTIVE` `PROACTIVE` È necessario specificare una modalità di valutazione e questo campo non può rimanere vuoto.

Per ulteriori informazioni, consulta Modalità di valutazione. Per un elenco di regole gestite che supportano la valutazione proattiva, vedere Elenco delle regole AWS Config gestite per modalità di valutazione.

> **Note**
>
> Le regole proattive non correggono le risorse contrassegnate come NON_COMPLIANT e non ne impediscono l'implementazione.

AWS Config struttura di regole personalizzata

Questa sezione contiene informazioni sull'utilizzo del AWS Config Rules Development Kit (RDK) e della AWS Config Rules Development Kit Library (RDKLib). Per ulteriori informazioni su RDK o RDKLib, consulta i repository e aws-config-rdklib. aws-config-rdk GitHub

Regole di scrittura

Prerequisiti

1. Segui la procedura descritta in Installazione di AWS CLI.
2. Segui i passaggi in Configurazione con la console o Configurazione con. AWS ConfigAWS ConfigAWS CLI Per informazioni sulle AWS regioni in cui AWS Config è supportato, seleziona la tua regione dall'elenco dei servizi AWS regionali.
3. Installa l'RDK usando il metodo consigliato con pip:

   ```
   pip install rdk
   ```

   > **Note**
   >
   > Prima di usare pip, assicurati che sia installato sul tuo computer.

4. Installa l'RDKLib usando il metodo consigliato con pip:

   ```
   pip install rdklib
   ```

   > **Note**
   >
   > Prima di usare pip, assicurati che sia installato sul tuo computer.

Regole attivate dalle modifiche

1. Per creare una regola attivata da una modifica al tipo di risorsa specificato, esegui il comando seguente:

```
rdk create YOUR_RULE_NAME --runtime python3.6-lib --resource-
types AWS::Resource::Type
```

L'esempio seguente crea una regola attivata da una modifica al tipo di risorsa `AWS::IAM::User`:

```
rdk create MFA_ENABLED_RULE --runtime python3.6-lib --resource-types AWS::IAM::User
```

Di seguito sono riportati i flag che è possibile utilizzare con il comando `rdk create` per le regole attivate dalle modifiche:

```
rdk create RULE_NAME
    --runtime pythonX.X-lib // Python runtime version
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
```

> **Note**
>
> Per utilizzare la RDKLib, il runtime della regola deve essere impostato su `python3.6-lib`.

Dopo l'esecuzione di `rdk create`, dovrebbe venire visualizzata una nuova directory con il nome della regola e 3 file al suo interno:

- *RULE_NAME*`.py`: file Python in cui è archiviata la logica della regola
- *RULE_NAME*`_test.py`: file Python in cui sono archiviati gli unit test della regola
- `parameters.json`: file JSON delle impostazioni di implementazione dell'RDK

2. La fase successiva consiste nella scrittura della logica della regola. Occorrerà solo modificare il file *RULE_NAME*.py. Aprendo il file *RULE_NAME*.py, vedrai un modello in cui è

possibile aggiungere la logica della regola. Di seguito è riportato il modello generato per MFA_ENABLED_RULE:

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ['AWS::IAM::User']

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ##############################
        # Add your custom logic here. #
        ##############################

        return [Evaluation(ComplianceType.NOT_APPLICABLE)]

    #def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
    #    pass

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

##############################
# DO NOT MODIFY ANYTHING BELOW #
##############################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

L'esempio seguente è una versione modificata del modello MFA_ENABLED_RULE con la logica della regola. La regola verifica se gli utenti IAM hanno abilitato l'autenticazione a più fattori (MFA). La regola è NON_COMPLIANT se un utente IAM non dispone dell'autenticazione a più fattori abilitata. Per ulteriori informazioni sulla logica delle regole e sui metodi forniti nel modello, consulta Logica della regola.

```
from rdklib import ComplianceType, ConfigRule, Evaluation, Evaluator

APPLICABLE_RESOURCES = ["AWS::IAM::User"]
```

```
class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):

        username = configuration_item.get("resourceName")

        iam_client = client_factory.build_client("iam")

        response = iam_client.list_mfa_devices(UserName=username)

        # Scenario:1 IAM user has MFA enabled.
        if response["MFADevices"]:
            return [Evaluation(ComplianceType.COMPLIANT)]

        # Scenario:2 IAM user has MFA not enabled.
        annotation = "MFA needs to be enabled for user."
        return [Evaluation(ComplianceType.NON_COMPLIANT, annotation=annotation)]

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

3. Il passaggio successivo consiste nell'installare il livello RDKLib AWS con la AWS console o. AWS CLI La RDKLib è progettata per funzionare come un livello AWS Lambda . Consente di utilizzare la libreria senza doverla includere nel pacchetto di implementazione.

   - Per installare il livello RDKLib con la AWS Console, procedi nel seguente modo:

     1. Apri la AWS Serverless Application Repository console all'indirizzo https://console.aws.amazon.com/serverlessrepo.
     2. Nel menu di navigazione a sinistra, scegli Applicazioni disponibili.
     3. Cerca `rdklib` e scegli rdklib.

4. Esamina i dettagli della funzione e poi passa all'implementazione. Non apportare alcuna modifica.
5. Nella sezione Risorse della pagina Panoramica, copia l'Amazon Resource Name (ARN) del layer Lambda. L'ARN del livello Lambda ti servirà quando implementi la regola.

- Per installare il livello RDKLib con AWS CLI, esegui i seguenti comandi:

1. Crea il set di modifiche per il livello RDKLib.

```
aws serverlessrepo create-cloud-formation-change-set --application-id
 arn:aws:serverlessrepo:ap-southeast-1:711761543063:applications/rdklib --
stack-name RDKlib-Layer
```

Verrà restituito l'output seguente:

```
{
    "ApplicationId": "arn:aws:serverlessrepo:ap-
southeast-1:711761543063:applications/rdklib",
    "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
a3d536322-585e-4ffd-9e2f-552c8b887d6f/ffe7ff5c-ab38-4ab9-b746-9c1617ca95c1",
    "SemanticVersion": "0.1.0",
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53"
}
```

2. Esegui il set di modifiche. È possibile copiare/incollare l'ARN completo del change-set ChangeSetId (dall'output generato nel passaggio precedente) per personalizzare il seguente comando:

```
aws cloudformation execute-change-set --change-set-name NAME_OF_THE_CHANGE_SET
```

3. Restituisce tutte le risorse associate che fanno parte dello stack implementato.

```
aws cloudformation describe-stack-resources --stack-name serverlessrepo-RDKlib-
Layer
```

Verrà restituito l'output seguente:

```
{
    "StackResources": [
        {
```

```
            "StackName": "serverlessrepo-RDKlib-Layer",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53",
            "LogicalResourceId": "RdklibLayercf22317faf",
            "PhysicalResourceId": "arn:aws:lambda:us-
east-1:123456789012:layer:rdklib-layer:1",
            "ResourceType": "AWS::Lambda::LayerVersion",
            "Timestamp": "2020-06-03T11:26:30.501Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "NOT_CHECKED"
            }
        }
    ]
}
```

4. Copia l'ARN del livello Lambda dall'output generato nel passaggio precedente. L'ARN del livello Lambda è il `PhysicalResourceId`.

```
"PhysicalResourceId": "arn:aws:lambda:us-east-1:123456789012:layer:rdklib-
layer:1"
```

4. Il passaggio successivo consiste nel fornire un ruolo che viene assunto dalla funzione Lambda. Per impostazione predefinita, le funzioni Lambda tentano di assumere il ruolo `AWSServiceRoleForConfig`, e questa è un'operazione non consentita. È necessario creare un ruolo con la policy gestita `AWS_ConfigRole`. Il ruolo deve avere una relazione di trust con AWS Config , e tutti i ruoli inclusi nel percorso /rdk/ devono assumere questo ruolo. Di seguito è illustrato un esempio di policy di attendibilità:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
```

```
        "AWS": "arn:aws:iam::account-ID:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": "arn:aws:iam::account-ID:role/rdk/*"
        }
      }
    }
  ]
}
```

Tramite questa policy di attendibilità, esegui il comando seguente:

```
aws iam create-role --role-name your-role-name --assume-role-policy-document
 file://trust-policy.json
```

Ora, esegui il comando seguente per aggiornare il parametro di input per `ExecutionRoleName` e specifica il nome del ruolo:

```
rdk modify YOUR_RULE_NAME --input-parameters '{"ExecutionRoleName":"your-role-
name"}'
```

È inoltre possibile utilizzare `rdk modify` per aggiornare i dettagli della regola attivata dalle modifiche utilizzando i seguenti flag:

```
rdk modify RULE_NAME
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
```

5. Il passaggio finale consiste nell'implementazione della regola. Per implementare la regola, esegui il comando seguente con l'ARN del livello Lambda del passaggio 3:

```
rdk deploy YOUR_RULE_NAME --rdklib-layer-arn YOUR_RDKLIB_LAYER_ARN
```

6. La regola è ora implementata. È possibile utilizzare la AWS Config console per verificare se la regola funziona come previsto.

Regole periodiche

1. Per creare una regola attivata periodicamente per un tipo di risorsa specificato, esegui il comando seguente:

```
rdk create YOUR_RULE_NAME --runtime python3.6-lib --resource-
types AWS::Resource::Type --maximum-frequency EXECUTION_FREQUENCY
```

L'esempio seguente crea una regola attivata ogni 24 ore per il tipo di risorsa `AWS::IAM::User`:

```
rdk create MFA_ENABLED_RULE --runtime python3.6-lib --resource-types AWS::IAM::User
 --maximum-frequency TwentyFour_Hours
```

Di seguito sono riportati i flag che è possibile utilizzare con il comando `rdk create` per le regole periodiche:

```
rdk create RULE_NAME
    --runtime pythonX.X-lib // Python runtime version
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
    --maximum-frequency EXECUTION_FREQUENCY // How often the rule should be run on
 a periodic trigger.
 One of ['One_Hour','Three_Hours','Six_Hours','Twelve_Hours','TwentyFour_Hours']
```

> **Note**
>
> Per utilizzare la RDKLib, il runtime della regola deve essere impostato su `python3.6-lib`.

Dopo l'esecuzione di `rdk create`, dovrebbe venire visualizzata una nuova directory con il nome della regola e 3 file al suo interno:

- *RULE_NAME*`.py`: file Python in cui è archiviata la logica della regola
- *RULE_NAME*`_test.py`: file Python in cui sono archiviati gli unit test della regola
- `parameters.json`: file JSON delle impostazioni di implementazione dell'RDK

2. La fase successiva consiste nella scrittura della logica della regola. Occorrerà solo modificare il file *RULE_NAME*.py. Aprendo il file *RULE_NAME*.py, vedrai un modello in cui è possibile aggiungere la logica della regola. Di seguito è riportato il modello generato per MFA_ENABLED_RULE:

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ['AWS::IAM::User']

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ##############################
        # Add your custom logic here. #
        ##############################

        return [Evaluation(ComplianceType.NOT_APPLICABLE)]

    #def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
    #    pass

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

Il modello utilizza per impostazione predefinita le regole attivate dalle modifiche. Invece, aggiungi la logica al metodo `evaluate_periodic`. L'esempio seguente è una versione modificata del modello MFA_ENABLED_RULE con la logica della regola. La regola verifica se gli utenti IAM hanno abilitato l'autenticazione a più fattori (MFA). La regola è NON_COMPLIANT se un utente IAM non dispone dell'autenticazione a più fattori abilitata. Per ulteriori informazioni sulla logica delle regole e sui metodi forniti nel modello, consulta Logica della regola.

```
from rdklib import ComplianceType, ConfigRule, Evaluation, Evaluator

APPLICABLE_RESOURCES = ["AWS::IAM::User"]

class MFA_ENABLED_RULE(ConfigRule):l

    def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
        evaluations = []

        iam_client = client_factory.build_client("iam")

        paginator = iam_client.get_paginator("list_users")
        response_iterator = paginator.paginate()

        for response in response_iterator:
            for user in response["Users"]:
                username = user["UserName"]
                response = iam_client.list_mfa_devices(UserName=username)

                # Scenario:1 IAM user has MFA enabled.
                if response["MFADevices"]:
                    evaluations.append(Evaluation(ComplianceType.COMPLIANT,
 username, "AWS::IAM::User"))

                # Scenario:2 IAM user has MFA not enabled.
                if not response["MFADevices"]:
                    annotation = "MFA needs to be enabled for user."
                    evaluations.append(
                        Evaluation(ComplianceType.NON_COMPLIANT, username,
 "AWS::IAM::User", annotation=annotation)
                    )
        return evaluations

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
```

```
    return evaluator.handle(event, context)
```

3. Il passaggio successivo consiste nell'installare il livello RDKLib AWS con la AWS Console o. AWS CLI La RDKLib è progettata per funzionare come un livello AWS Lambda . Consente di utilizzare la libreria senza doverla includere nel pacchetto di implementazione.

   - Per installare il livello RDKLib con la AWS Console, procedi nel seguente modo:

     1. Apri la AWS Serverless Application Repository console all'indirizzo https://console.aws.amazon.com/serverlessrepo.
     2. Nel menu di navigazione a sinistra, scegli Applicazioni disponibili.
     3. Cerca `rdklib` e scegli rdklib.
     4. Esamina i dettagli della funzione e poi passa all'implementazione. Non apportare alcuna modifica.
     5. Nella sezione Risorse della pagina Panoramica, copia l'Amazon Resource Name (ARN) del layer Lambda. L'ARN del livello Lambda ti servirà quando implementi la regola.

   - Per installare il livello RDKLib con AWS CLI, esegui i seguenti comandi:

     1. Crea il set di modifiche per il livello RDKLib.

        ```
        aws serverlessrepo create-cloud-formation-change-set --application-id
         arn:aws:serverlessrepo:ap-southeast-1:711761543063:applications/rdklib --
        stack-name RDKlib-Layer
        ```

        Verrà restituito l'output seguente:

        ```
        {
            "ApplicationId": "arn:aws:serverlessrepo:ap-
        southeast-1:711761543063:applications/rdklib",
            "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
        a3d536322-585e-4ffd-9e2f-552c8b887d6f/ffe7ff5c-ab38-4ab9-b746-9c1617ca95c1",
            "SemanticVersion": "0.1.0",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
        serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53"
        }
        ```

     2. Esegui il set di modifiche. È possibile copiare/incollare l'ARN completo del change-set ChangeSetId (dall'output generato nel passaggio precedente) per personalizzare il seguente comando:

```
aws cloudformation execute-change-set --change-set-name NAME_OF_THE_CHANGE_SET
```

3. Restituisce tutte le risorse associate che fanno parte dello stack implementato.

```
aws cloudformation describe-stack-resources --stack-name serverlessrepo-RDKlib-
Layer
```

Verrà restituito l'output seguente:

```
{
    "StackResources": [
        {
            "StackName": "serverlessrepo-RDKlib-Layer",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53",
            "LogicalResourceId": "RdklibLayercf22317faf",
            "PhysicalResourceId": "arn:aws:lambda:us-
east-1:123456789012:layer:rdklib-layer:1",
            "ResourceType": "AWS::Lambda::LayerVersion",
            "Timestamp": "2020-06-03T11:26:30.501Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "NOT_CHECKED"
            }
        }
    ]
}
```

4. Copia l'ARN del livello Lambda dall'output generato nel passaggio precedente. L'ARN del livello Lambda è il `PhysicalResourceId`.

```
"PhysicalResourceId": "arn:aws:lambda:us-east-1:123456789012:layer:rdklib-
layer:1"
```

4. Il passaggio successivo consiste nel fornire un ruolo che viene assunto dalla funzione Lambda. Per impostazione predefinita, le funzioni Lambda tentano di assumere il ruolo `AWSServiceRoleForConfig`, e questa è un'operazione non consentita. È necessario creare un ruolo con la policy gestita `AWS_ConfigRole`. Il ruolo deve avere una relazione di trust con AWS Config , e tutti i ruoli inclusi nel percorso /rdk/ devono assumere questo ruolo. Di seguito è illustrato un esempio di policy di attendibilità:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-ID:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": "arn:aws:iam::account-ID:role/rdk/*"
        }
      }
    }
  ]
}
```

Tramite questa policy di attendibilità, esegui il comando seguente:

```
aws iam create-role --role-name your-role-name --assume-role-policy-document
 file://trust-policy.json
```

Ora, esegui il comando seguente per aggiornare il parametro di input per `ExecutionRoleName` e specifica il nome del ruolo:

```
rdk modify YOUR_RULE_NAME --input-parameters '{"ExecutionRoleName":"your-role-
name"}'
```

È inoltre possibile utilizzare `rdk modify` per aggiornare i dettagli della regola periodica utilizzando i seguenti flag:

```
rdk modify RULE_NAME
```

```
   --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
   --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
   --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
   --maximum-frequency EXECUTION_FREQUENCY // How often the rule should be run on
 a periodic trigger.
 One of ['One_Hour','Three_Hours','Six_Hours','Twelve_Hours','TwentyFour_Hours']
```

5. Il passaggio finale consiste nell'implementazione della regola. Per implementare la regola, esegui il comando seguente con l'ARN del livello Lambda del passaggio 3:

```
rdk deploy YOUR_RULE_NAME --rdklib-layer-arn YOUR_RDKLIB_LAYER_ARN
```

6. La regola è ora implementata. È possibile utilizzare la AWS Config console per verificare se la regola funziona come previsto.

Logica della regola

Il seguente esempio di codice Python è un modello per la scrittura di una regola tramite l'RDK e la RDKLib. Occorre apportare le modifiche solo all'interno dei metodi `evaluate_parameters`, `evaluate_change` e `evaluate_periodic` o scrivere funzioni completamente nuove per facilitare la logica, se necessario. Per i prerequisiti per la scrittura delle regole con l'RDK e la RDKLib, consulta Prerequisiti.

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ["AWS::Resource::Type"]

# When you create a rule, the class name will be the name you give the rule when you
 create it instead of ConfigRule
class ConfigRule (ConfigRule):

    def evaluate_parameters(self, rule_parameters):
        return rule_parameters

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ###############################
        # Add your custom logic here. #
        ###############################
```

```
    def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
        ##############################
        # Add your custom logic here. #
        ##############################

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = ConfigRule()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

APPLICABLE_RESOURCES

`APPLICABLE_RESOURCES` sono i tipi di risorsa a cui è indirizzata la regola. Se utilizzate, devono essere una variabile globale impostata sui tipi di risorsa a cui la regola è indirizzata. Per un elenco di tipi di risorsa supportati, consulta Tipi di risorsa supportati.

evaluate_parameters

Descrizione

Questo metodo viene utilizzato per verificare se i parametri di input della regola sono validi. Di seguito sono riportate le best practice:

- Verifica se è elencato il numero corretto di parametri.
- Verifica se il nome del parametro è corretto.
- Verifica se il valore del parametro è del tipo corretto.
- Se il parametro è un numero intero, verifica se è compreso tra limiti ragionevoli.
- Se il parametro ha un numero limitato di opzioni possibili, verifica se il parametro è una di quelle opzioni.
- Se il parametro è di tipo Stringa, verifica se è di una lunghezza ragionevole e ritaglia lo spazio prima o dopo il valore.
- Verifica se la distinzione tra maiuscole e minuscole viene gestita in modo appropriato.
- Limita l'immissione dei parametri quando possibile. Ad esempio, se ricevi un elenco di ARN separato da virgole, assicurati che gli unici caratteri consentiti siano le virgole e i caratteri supportati dagli ARN.

Parametri

`rule_parameters` è un dizionario dei parametri di input della regola.

Sintassi di ritorno

Se uno dei parametri non è valido, puoi generare un errore `InvalidParametersError`:

```
from rdklib import InvalidParametersError
raise InvalidParametersError("Error message to display")
```

Se i parametri sono tutti validi, il metodo dovrebbe restituire un dizionario:

```
return valid_rule_parameters
```

evaluate_change

Descrizione

Questo metodo viene utilizzato per la logica di valutazione di una regola attivata dalle modifiche.

Parametri

`event`è l' AWS Lambda evento fornito da AWS Config. È un documento in formato JSON formattato che contiene i dati che una funzione Lambda deve elaborare. Per esempi, vedi Eventi di esempio per AWS Config le regole.

`client_factory`è l' ClientFactory oggetto da utilizzare per la regola. La ClientFactory classe crea o riutilizza un client boto3, che fornisce un'interfaccia di basso livello a un servizio. AWS I metodi client boto3 vengono mappati con un'API di AWS servizio, il che significa che le operazioni di servizio vengono mappate ai metodi client con lo stesso nome e forniscono l'accesso agli stessi parametri operativi. Per un elenco dei servizi disponibili, consulta Servizi disponibili nella documentazione Boto3.

La sintassi della richiesta di `client_factory` è la seguente:

```
response = client_factory.build_client(
    service='string')
```

Per esempio:

```
iam_client = client_factory.build_client("iam")
```

> **Note**
>
> Il nome boto3 del servizio è obbligatorio. AWS

`configuration_item` è il dizionario dell'elemento di configurazione completo, anche se sovradimensionato. Un elemento di configurazione rappresenta una point-in-time visualizzazione dei vari attributi di una risorsa supportata AWS . Per informazioni sul contenuto di`ConfigurationItem`, consulta ConfigurationItemI' AWS Config API Reference.

`valid_rule_parameters` è l'output del metodo `evaluate_parameters()`.

Sintassi di ritorno

Il metodo deve restituire uno o più dei seguenti elementi:

```
[Evaluation(ComplianceType.COMPLIANT)]
```

```
[Evaluation(ComplianceType.NON_COMPLIANT)]
```

```
[Evaluation(ComplianceType.NOT_APPLICABLE)]
```

> **Note**
>
> Le regole che segnalano le risorse eliminate devono restituire il risultato della valutazione di `NOT_APPLICABLE` per evitare valutazioni non necessarie delle regole.

È necessario utilizzare le annotazioni per tutte le valutazioni non conformi. Per esempio:

```
[return [Evaluation(ComplianceType.NON_COMPLIANT, annotation="Explanation for why
 the rule is NON_COMPLIANT")]]
```

evaluate_periodic

Descrizione

Questo metodo viene utilizzato per valutare una regola periodica.

Parametri

`event`è l'evento fornito da. AWS Lambda AWS ConfigÈ un documento in formato JSON formattato che contiene i dati che una funzione Lambda deve elaborare. Per esempi, vedi Eventi di esempio per AWS Config le regole.

`client_factory`è l' ClientFactory oggetto da utilizzare per la regola. La ClientFactory classe crea o riutilizza un client boto3, che fornisce un'interfaccia di basso livello a un servizio. AWS I metodi client boto3 vengono mappati con un'API di AWS servizio, il che significa che le operazioni di servizio vengono mappate ai metodi client con lo stesso nome e forniscono l'accesso agli stessi parametri operativi. Per un elenco dei servizi disponibili, consulta Servizi disponibili nella documentazione Boto3.

La sintassi della richiesta di `client_factory` è la seguente:

```
response = client_factory.build_client(
    service='string')
```

Per esempio:

```
iam_client = client_factory.build_client("iam")
```

> **Note**
>
> Il nome boto3 del servizio è obbligatorio. AWS

`valid_rule_parameters` è l'output del metodo `evaluate_parameters()`.

Sintassi di ritorno

Il metodo deve restituire uno o più dei seguenti elementi:

```
[Evaluation(ComplianceType.COMPLIANT)]
```

```
[Evaluation(ComplianceType.NON_COMPLIANT)]
```

```
[Evaluation(ComplianceType.NOT_APPLICABLE)]
```

> **Note**
>
> Le regole che segnalano le risorse eliminate devono restituire il risultato della valutazione di `NOT_APPLICABLE` per evitare valutazioni non necessarie delle regole.

È necessario utilizzare le annotazioni per tutte le valutazioni non conformi. Per esempio:

```
[return [Evaluation(ComplianceType.NON_COMPLIANT, annotation="Explanation for why
 the rule is NON_COMPLIANT")]]
```

lambda_handler

Descrizione

Non dovrebbe essere necessario modificare questo metodo. Il gestore lambda viene utilizzato per elaborare gli eventi. La funzione viene eseguita quando AWS Lambda passa l'`event`oggetto al metodo. `handler` Per ulteriori informazioni, consulta Gestore della funzione Lambda in Python.

Parametri

`event`è l' AWS Lambda evento fornito da AWS Config. È un documento in formato JSON formattato che contiene i dati che una funzione Lambda deve elaborare. Per esempi, vedi Eventi di esempio per AWS Config le regole.

`context` è un oggetto passato alla funzione da Lambda durante il runtime. Questo oggetto specifica i metodi e le proprietà che forniscono le informazioni e i metodi che la funzione può utilizzare durante l'esecuzione. Tieni presente che nelle versioni più recenti di Lambda il contesto non è più utilizzato.

Modalità di valutazione e tipi di trigger per AWS Config le regole

Quando aggiungi una regola al tuo account, puoi specificare in che momento del processo di creazione e gestione delle risorse desideri AWS Config valutare le tue risorse. Il processo di creazione e gestione delle risorse è noto come provisioning delle risorse. Scegliete la modalità di

valutazione per specificare quando, in questo processo, desiderate AWS Config valutare le vostre risorse.

A seconda della regola, è AWS Config possibile valutare le configurazioni delle risorse prima che una risorsa venga distribuita, dopo la distribuzione di una risorsa o entrambe le cose. La valutazione di una risorsa prima che venga implementata è chiamata valutazione proattiva. La valutazione di una risorsa dopo che è stata implementata è chiamata valutazione dei test.

Puoi scegliere anche il tipo di trigger per specificare la frequenza con cui le regole AWS Config valutano le risorse. Le risorse possono essere valutate in caso di modifiche alla configurazione, in base a una pianificazione periodica o in entrambi i casi.

Tipi di trigger

Dopo aver aggiunto una regola al tuo account, AWS Config confronta le tue risorse con le condizioni della regola. Dopo questa valutazione iniziale, AWS Config continua a eseguire le valutazioni ogni volta che ne viene attivata una. Gli eventi scatenanti della valutazione sono definiti come parte della regola e possono includere le seguenti tipologie:

Tipo di trigger	Descrizione
Modifiche di configurazione	AWS Config esegue le valutazioni della regola quando esiste una risorsa che corrisponde all'ambito della regola e c'è una modifica nella configurazione della risorsa. La valutazione viene eseguita dopo l' AWS Config invio di una notifica di modifica dell'elemento di configura zione. Puoi scegliere le risorse che avviano la valutazione definendo l'ambito della regola. L'ambito può includere quanto segue: • Uno o più tipi di risorse • Una combinazione di un tipo di risorsa e un ID risorsa • Una combinazione di una chiave e un valore di un tag

Tipo di trigger	Descrizione
	• Quando viene creata, aggiornata o eliminata qualsiasi risorsa registrata AWS Config esegue la valutazione quando rileva una modifica a una risorsa che corrispon de all'ambito della regola. Puoi utilizzare l'ambito per definire le risorse che avviano le valutazioni.
Periodic (Periodico)	AWS Config esegue le valutazioni della regola con una frequenza scelta dall'utente, ad esempio ogni 24 ore.
Ibrido	Alcune regole prevedono sia trigger legati alle modifiche alla configurazione che trigger periodici. Per queste regole, AWS Config valuta le risorse quando rileva una modifica della configurazione e anche alla frequenza specifica ta.

Modalità di valutazione

Esistono due modalità di valutazione:

Modalità proattiva

Utilizza la valutazione proattiva per valutare le risorse prima che vengano implementate. Ciò consente di valutare se un insieme di proprietà delle risorse, se utilizzato per definire una AWS risorsa, sarebbe CONFORME o NON CONFORME, in base all'insieme di regole proattive che hai nel tuo account nella tua regione.

Lo schema del tipo di risorsa indica le proprietà di una risorsa. Puoi trovare lo schema del tipo di risorsa nelle "estensioni AWS pubbliche" all'interno del AWS CloudFormation registro o con il seguente comando CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Per ulteriori informazioni, consulta Gestione delle estensioni tramite il AWS CloudFormation registro e il riferimento ai tipi di AWS risorse e proprietà nella Guida per l' AWS CloudFormation utente.

> **Note**
>
> Le regole proattive non correggono le risorse contrassegnate come NON_COMPLIANT e non ne impediscono l'implementazione.

Elenco di regole gestite con valutazione proattiva

Per un elenco delle regole gestite che supportano la valutazione proattiva, vedere Elenco delle regole AWS Config gestite per modalità di valutazione.

Elenco dei tipi di risorse supportati per la valutazione proattiva

Di seguito è riportato un elenco dei tipi di risorse supportati per la valutazione proattiva:

- `AWS::ApiGateway::Stage`
- `AWS::AutoScaling::AutoScalingGroup`
- `AWS::EC2::EIP`
- `AWS::EC2::Instance`
- `AWS::EC2::Subnet`
- `AWS::Elasticsearch::Domain`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::Redshift::Cluster`
- `AWS::S3::Bucket`
- `AWS::SNS::Topic`

Regola di esempio con valutazione proattiva

Regola proattiva di esempio

1. Aggiungi la regola AWS Config gestita al tuo account per verificare se i bucket S3 hanno la registrazione abilitata. `S3_BUCKET_LOGGING_ENABLED`

2. Per la modalità di valutazione, scegli Attiva la valutazione proattiva nella console di AWS gestione o abilita `PROACTIVE` per `EvaluationModes` nell'API. PutConfigRule

Dopo aver attivato la valutazione proattiva, puoi utilizzare l'StartResourceEvaluationAPI e l'GetResourceEvaluationSummaryAPI per verificare se in un bucket del tuo account, che non è stato distribuito in produzione, non è abilitata la registrazione. Ciò consente di testare le configurazioni delle risorse prima dell'implementazione e di rivalutare se desideri distribuire la risorsa in produzione.

Ad esempio, inizia con l'API: StartResourceEvaluation

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::S3::Bucket",
                                     "ResourceConfiguration": "{\"BucketName\": \"my-
bucket\", \"LoggingConfiguration\": {\"DestinationBucketName\": \"my-log-bucket\",
\"LogFilePrefix\":\"my-log\"}}",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Viene visualizzato `ResourceEvaluationId` nell'output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Quindi, utilizza `ResourceEvaluationId` con l' GetResourceEvaluationSummary API per verificare il risultato della valutazione:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Riceverai un output simile al seguente:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
```

```
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration": "{\"BucketName\": \"my-bucket\",
 \"LoggingConfiguration\": {\"DestinationBucketName\": \"my-log-bucket\",
\"LogFilePrefix\":\"my-log\"}}",

    }
}
```

Per visualizzare informazioni aggiuntive sul risultato della valutazione, ad esempio la regola che ha contrassegnato una risorsa come NON_COMPLIANT, utilizza l'API. GetComplianceDetailsByResource

Modalità di test

Utilizza la valutazione di test per valutare le risorse che sono già state implementate. Ciò consente di valutare le impostazioni di configurazione delle risorse esistenti.

Regole di esempio con valutazione di test

Esempio di regola attivata dalle modifiche

1. Aggiungi la regola gestita, `S3_BUCKET_LOGGING_ENABLED`, all'account per verificare se la registrazione di log è abilitata per i bucket S3.
2. Il tipo di trigger per la regola sono le modifiche alla configurazione. AWS Config esegue le valutazioni della regola quando un bucket S3 viene creato, modificato o eliminato.
3. Quando un bucket viene aggiornato, la modifica alla configurazione avvia la regola e AWS Config valuta se il bucket è conforme rispetto a quest'ultima.

Esempio di regola periodica

1. Aggiungi la regola gestita, `IAM_PASSWORD_POLICY`, all'account. La regola verifica se la policy delle password per gli utenti IAM è conforme alla policy del tuo account, ad esempio, se richiede una lunghezza minima o caratteri specifici.
2. Il tipo di trigger per la regola è periodico. AWS Config esegue la valutazione della regola con una frequenza specificata, ad esempio ogni 24 ore.

3. Ogni 24 ore, la regola viene avviata e AWS Config valuta se le password degli utenti IAM sono conformi alla regola.

Esempio di regola ibrida con trigger periodici e di modifica alla configurazione

1. Crea una regola personalizzata che valuti se i AWS CloudTrail percorsi del tuo account sono attivi e se la registrazione è valida per tutte le regioni.
2. Vuoi AWS Config eseguire le valutazioni della regola ogni volta che un percorso viene creato, aggiornato o eliminato. Inoltre, desideri AWS Config eseguire la regola ogni 12 ore.
3. Per il tipo di trigger, scrivi la logica sia per il trigger di modifica alla configurazione e per il trigger periodico. Per ulteriori informazioni, consulta Componenti di una AWS Config regola: regole di scrittura.

Valutazioni delle regole quando il registratore della configurazione è spento

Se si spegne il registratore di configurazione, AWS Config interrompe la registrazione delle modifiche alle configurazioni delle risorse. Ciò influisce sulle valutazioni delle regole nei seguenti modi:

- Le regole periodiche continuano a eseguire valutazioni alla frequenza specificata.
- Le regole attivate dalle modifiche non eseguono valutazioni.
- Le regole ibride eseguono le valutazioni solo alla frequenza specificata. Le regole non eseguono le valutazioni per le modifiche delle configurazioni.
- Se esegui una valutazione on demand per una regola con un trigger di modifica alla configurazione, la regola valuta l'ultimo stato conosciuto della risorsa, ovvero l'ultimo elemento di configurazione registrato.

> **Important**
>
> Evitate valutazioni non necessarie AWS Config
> Le regole periodiche e le regole ibride continuano ad essere eseguite, a meno che non vengano eliminate, anche se hai disattivato il registratore di configurazione. Queste regole valutano solo gli elementi di configurazione che sono stati registrati prima della disattivazione del registratore di configurazione, il che significa che riproducono gli stessi risultati di valutazione senza nuove informazioni. Elimina le regole periodiche e le regole ibride quando

disattivi il registratore di configurazione per evitare attività e valutazioni delle regole non necessarie.

AWS Config Regole gestite

AWS Config fornisce regole AWS gestite, che sono regole predefinite e personalizzabili che vengono AWS Config utilizzate per valutare se le AWS risorse sono conformi alle migliori pratiche comuni. Ad esempio, puoi utilizzare una regola gestita per valutare in modo rapido se i volumi Amazon Elastic Block Store (Amazon EBS) vengono crittografati o se alle risorse sono applicati tag specifici. La AWS Config console guida l'utente attraverso il processo di configurazione e attivazione di una regola gestita. Puoi anche utilizzare l' AWS Config API AWS Command Line Interface or per passare il codice JSON che definisce la configurazione di una regola gestita.

Puoi inoltre personalizzare il comportamento di una regola gestita per adattarlo alle tue esigenze. Ad esempio, potresti definire l'ambito della regola in modo da vincolare le risorse in grado di attivare una valutazione della regola, come ad esempio le istanze o i volumi di EC2. Hai la possibilità di personalizzare i parametri della regola per definire gli attributi che le risorse devono avere per soddisfare la regola. Ad esempio, puoi personalizzare un parametro in modo da specificare che il gruppo di sicurezza deve bloccare il traffico in entrata per un determinato numero di porta.

Considerazioni sui costi

Per informazioni dettagliate sui costi associati alla registrazione delle risorse, consulta la pagina AWS Config dei prezzi.

Consiglio: interrompi la registrazione della conformità delle risorse prima di eliminare le regole

Si consiglia vivamente di interrompere la registrazione per il tipo di `AWS::Config::ResourceCompliance` risorsa prima di eliminare le regole nell'account. L'eliminazione delle regole crea elementi di configurazione (CI) `AWS::Config::ResourceCompliance` e può influire sui costi del registratore AWS Config di configurazione. Se si eliminano regole che valutano un gran numero di tipi di risorse, ciò può portare a un picco nel numero di CI registrati.

Procedura ottimale:

1. Interrompi la registrazione `AWS::Config::ResourceCompliance`
2. Eliminare regole

3. Attiva la registrazione per `AWS::Config::ResourceCompliance`

Tipi di trigger

Dopo aver aggiunto una regola al tuo account, AWS Config confronta le tue risorse con le condizioni della regola. Dopo questa valutazione iniziale, AWS Config continua a eseguire le valutazioni ogni volta che ne viene attivata una. I trigger di valutazione sono definiti come parte della regola e possono includere i seguenti tipi.

Tipo di trigger	Descrizione
Modifiche di configurazione	AWS Config esegue le valutazioni della regola quando esiste una risorsa che corrisponde all'ambito della regola e c'è una modifica nella configurazione della risorsa. La valutazione viene eseguita dopo l' AWS Config invio di una notifica di modifica dell'elemento di configura zione. Puoi scegliere le risorse che avviano la valutazione definendo l'ambito della regola. L'ambito può includere quanto segue: • Uno o più tipi di risorse • Una combinazione di un tipo di risorsa e un ID risorsa • Una combinazione di una chiave e un valore di un tag • Quando viene creata, aggiornata o eliminata qualsiasi risorsa registrata AWS Config esegue la valutazione quando rileva una modifica a una risorsa che corrispon

Tipo di trigger	Descrizione
	de all'ambito della regola. Puoi utilizzare l'ambito per definire le risorse che avviano le valutazioni.
Periodic (Periodico)	AWS Config esegue le valutazioni della regola con una frequenza scelta dall'utente, ad esempio ogni 24 ore.
Ibrido	Alcune regole prevedono sia trigger legati alle modifiche alla configurazione che trigger periodici. Per queste regole, AWS Config valuta le risorse quando rileva una modifica della configurazione e anche alla frequenza specifica ta.

Modalità di valutazione

Esistono due modalità di valutazione delle AWS Config regole.

Modalità di valutazione	Descrizione
Proattiva	Utilizza la valutazione proattiva per valutare le risorse prima che vengano implementate. Ciò consente di valutare se un insieme di proprietà della risorsa, se utilizzato per definire una AWS risorsa, sarebbe CONFORME o NON CONFORME, in base all'insieme di regole proattive che hai nel tuo account nella tua regione. Per ulteriori informazioni, consulta Modalità di valutazione. Per un elenco di regole gestite che supportano la valutazione proattiva, vedi Elenco delle regole gestite per modalità di valutazione. AWS Config

Modalità di valutazione	Descrizione
Test	Utilizza la valutazione di test per valutare le risorse che sono già state implementate. Ciò consente di valutare le impostazioni di configurazione delle risorse esistenti.

> **Note**
>
> Le regole proattive non correggono le risorse contrassegnate come NON_COMPLIANT e non ne impediscono l'implementazione.

Argomenti

- Elenco di regole AWS Config gestite
- Elenco di regole AWS Config gestite per modalità di valutazione
- Elenco di regole AWS Config gestite per tipo di trigger
- Elenco delle regole AWS Config gestite per disponibilità regionale
- Regole collegate ai servizi AWS Config
- Creazione di regole gestite di AWS Config con modelli AWS CloudFormation

Elenco di regole AWS Config gestite

AWS Config attualmente supporta le seguenti regole gestite.

Considerazioni

Valori predefiniti per le regole gestite

I valori predefiniti specificati per le regole gestite sono precompilati solo quando si utilizza la console. AWS I valori predefiniti non sono forniti per l'API, la CLI o l'SDK.

I bucket di directory non sono supportati

Le regole gestite supportano solo bucket generici durante la valutazione delle risorse di Amazon Simple Storage Service (Amazon S3). AWS Config non registra le modifiche alla configurazione per i

bucket di directory. Per ulteriori informazioni sui bucket generici e sui bucket di directory, consulta la panoramica dei bucket e bucket di directory nella guida utente di Amazon S3.

Regole gestite e tipi di risorse IAM globali

I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.

Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.

Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.

Argomenti

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check

- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check

- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloudtrail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled

- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-iam-abilitato all'autorizzazione
- abilitato per dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled

- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-systems-manager
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted

- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory

- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile-pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-crittografato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled

- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- abilitato al controllo di protezione guardduty-eks
- abilitato per guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty
- guardduty - abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds

- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- controllo della scadenza del certificato iam-server
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- restricted-ssh
- abilitato a inspector-ec2-scan
- abilitato a Inspector-ecr-scan
- abilitato alla scansione del codice lambda dell'ispettore
- inspector-lambda-standard-scan abilitato
- ec2-instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-criptato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloudtrail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled

- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check

- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso alle porte senza restrizioni
- required-tags
- restricted-common-ports
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited

- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica tra più regioni con bucket s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo dei servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-noftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo della restrizione della porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty

- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

access-keys-rotated

Verifica se le chiavi di accesso IAM attive vengono ruotate (cambiate) entro il numero di giorni specificato in `maxAccessKeyAge`. La regola è NON_COMPLIANT se le chiavi di accesso non vengono ruotate entro il periodo di tempo specificato. Il valore predefinito è 90 giorni.

> **Warning**
>
> Non fornire le chiavi di accesso a parti non autorizzate, neppure per contribuire a trovare gli identificatori di account. Se lo facessi, daresti a qualcuno accesso permanente al tuo account. La sicurezza delle best practice consiste nel rimuovere le password e le chiavi di accesso quando gli utenti non ne hanno più bisogno.

> **Note**
>
> Tipo di risorsa contrassegnato come non conforme nella console
> Se questa regola rileva che una delle chiavi di accesso non è conforme, anche il tipo di `AWS::IAM::User` risorsa verrà contrassegnato come non conforme nella console. AWS Regole gestite e tipi di risorse IAM globali
> I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`AWS::IAM::Role, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.
> Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le

regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.
Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.
Limitazioni
Questa regola non si applica alle chiavi di accesso degli utenti root dell' AWS account. Per eliminare o ruotare le chiavi di accesso dell'utente root, utilizza le credenziali dell'utente root per accedere alla pagina Le mie credenziali di sicurezza all'indirizzo. AWS Management Console https://aws.amazon.com/console/

Identifier (Identificatore): ACCESS_KEYS_ROTATED

Tipi di risorse: AWS::IAM::User

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

AccessKeyEtà massima, Tipo: int, Impostazione predefinita: 90

Numero massimo di giorni senza rotazione. Impostazione predefinita: 90.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

account-part-of-organizations

Verifica se un AWS account fa parte di AWS Organizations. La regola è NON_COMPLIANT se un AWS account non fa parte di Organizations AWS o l'ID dell'account principale di AWS Organizations non corrisponde al parametro della regola. `MasterAccountId`

> **Note**
>
> Regole gestite e tipi di risorse IAM globali

I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.

Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.

Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.

Identificatore: ACCOUNT_PART_OF_ORGANIZATIONS

Tipo di trigger: Periodico

Regione AWS: tutte le AWS regioni supportate

Parametri:

MasterAccountId (Facoltativo), ▬Tipo: stringa

L'ID dell'account principale di un AWS account.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

acm-certificate-expiration-check

Verifica se i certificati AWS Certificate Manager presenti nel tuo account sono contrassegnati per scadere entro il numero di giorni specificato. I certificati forniti da ACM vengono rinnovati automaticamente. ACM non rinnova automaticamente i certificati importati. La regola è NON_COMPLIANT se i certificati sono vicini alla scadenza.

Identificatore: ACM_CERTIFICATE_EXPIRATION_CHECK

Tipi di risorse: AWS::ACM::Certificate

Tipo di trigger: Modifiche alla configurazione e periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

daysToExpiration (Facoltativo), Tipo: int, Impostazione predefinita: 14

> Specifica il numero di giorni prima che la regola contrassegni il certificato ACM come non conforme.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

acm-certificate-rsa-check

Verifica se i certificati RSA gestiti da AWS Certificate Manager (ACM) hanno una lunghezza di chiave di almeno «2048» bit. La regola è NON_COMPLIANT se la lunghezza minima della chiave è inferiore a 2048 bit.

Identificatore: ACM_CERTIFICATE_RSA_CHECK

Tipi di risorse: AWS::ACM::Certificate

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

acm-pca-root-ca-disabled

Verifica se l'Autorità di certificazione AWS AWS privata (CA privata) ha una CA radice disabilitata. La regola è NON_COMPLIANT per le CA root con stato diverso da DISABLED.

Identificatore: ACM_PCA_ROOT_CA_DISABLED

Tipi di risorse: AWS::ACMPCA::CertificateAuthority

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

exemptedCAArns (opzionale), Tipo: CSV

> Elenco separato da virgole dei nomi della risorsa Amazon (ARN) delle CA che è possibile abilitare. Questo valore può essere fornito per altre CA, come CA root specifiche o CA intermedie che possono essere abilitate.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

alb-desync-mode-check

Verifica se un Application Load Balancer (ALB) è configurato con una modalità di mitigazione desincronizzata definita dall'utente. La regola è NON_COMPLIANT se la modalità di mitigazione desincronizzata dell'ALB non corrisponde alla modalità di mitigazione desincronizzata definita dall'utente.

Identificatore: ALB_DESYNC_MODE_CHECK

Tipi di risorse: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

desyncMode, Tipo: CSV

Elenco separato da virgole in cui i clienti possono scegliere un massimo di 2 valori tra: "defensive", "strictest" e "monitor".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

alb-http-drop-invalid-header-enabled

Verifica se la regola valuta gli AWS Application Load Balancer (ALB) per assicurarsi che siano configurati per eliminare le intestazioni http. La regola è NON_COMPLIANT se il valore di routing.http.drop_invalid_header_fields.enabled è impostato su false.

Identificatore: ALB_HTTP_DROP_INVALID_HEADER_ENABLED

Tipi di risorse: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

alb-http-to-https-redirection-check

Verifica se il reindirizzamento da HTTP a HTTPS è configurato su tutti gli ascoltatori HTTP degli Application Load Balancer. La regola è NON_COMPLIANT se il reindirizzamento da HTTP a HTTPS non è configurato per uno o più ascoltatori HTTP dell'Application Load Balancer. La regola è NON_COMPLIANT anche se uno o più ascoltatori HTTP esegue l'inoltro a un ascoltatore HTTP invece del reindirizzamento.

Identificatore: ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

Tipi di risorse: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

alb-waf-enabled

Verifica se AWS WAF è abilitato su Application Load Balancers (ALBs). La regola è NON_COMPLIANT se key: waf.enabled è impostato su false.

Identificatore: ALB_WAF_ENABLED

Tipi di risorse: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

waf WebAclIds (opzionale), Tipo: CSV

Elenco separato da virgole degli ID dell'ACL Web (per WAF) o degli ARN dell'ACL Web (per WAFV2) per la verifica dell'associazione ALB.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

api-gwv2-access-logs-enabled

Verifica se la registrazione di log degli accessi è abilitata per tutte le fasi di Gateway Amazon API V2. La regola è NON_COMPLIANT se «access» non è presente nella configurazione dello stage. LogSettings

Identificatore: API_GWV2_ACCESS_LOGS_ENABLED

Tipi di risorse: AWS::ApiGatewayV2::Stage

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

api-gwv2-authorization-type-configured

Verifica se per i percorsi API di Gateway Amazon API v2 è impostato un tipo di autorizzazione. Questa regola è NON_COMPLIANT se il tipo di autorizzazione è NONE.

Identificatore: API_GWV2_AUTHORIZATION_TYPE_CONFIGURED

Tipi di risorse: AWS::ApiGatewayV2::Route

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

authorizationType (opzionale), ▪Tipo: stringa

Parametro in base a cui verificare i tipi di autorizzazione dei percorsi API. I parametri di stringa che corrispondono a CUSTOM, AWS_IAM, JWT sono validi.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

api-gw-associated-with-waf

Verifica se una fase API di Amazon API Gateway utilizza una lista di controllo degli accessi Web AWS WAF (Web ACL). La regola è NON_COMPLIANT se non viene utilizzato un ACL Web AWS WAF o se un ACL AWS Web utilizzato non corrisponde a quanto elencato nel parametro della regola.

Identificatore: API_GW_ASSOCIATED_WITH_WAF

Tipi di risorse: AWS::ApiGateway::Stage

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

WebAclArns (Facoltativo), Tipo: CSV

Elenco separato da virgole dei nomi della risorsa Amazon (ARN) dell'ACL Web.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

api-gw-cache-enabled-and-encrypted

Verifica se la cache di tutti i metodi nelle fasi di Gateway Amazon API è abilitata e crittografata. La regola è NON_COMPLIANT se un metodo in una fase di Gateway Amazon API non è configurato per la cache o se la cache non è crittografata.

Identificatore: API_GW_CACHE_ENABLED_AND_ENCRYPTED

Tipi di risorse: AWS::ApiGateway::Stage

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

api-gw-endpoint-type-check

Verifica se le API di Gateway Amazon API sono del tipo specificato nel parametro della regola `endpointConfigurationType`. La regola restituisce NON_COMPLIANT se REST API non corrisponde al tipo di endpoint configurato nel parametro della regola.

Identifier: API_GW_ENDPOINT_TYPE_CHECK

Tipi di risorse: AWS::ApiGateway::RestApi

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

endpoint ConfigurationTypes, ▬Tipo: stringa

Elenco separato da virgole dei permessi. endpointConfigurationTypes I valori consentiti sono REGIONAL, PRIVATE ed EDGE.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

api-gw-execution-logging-enabled

Verifica se la registrazione di log è abilitata per tutti i metodi nelle fasi di Gateway Amazon API. La regola è NON_COMPLIANT se la registrazione di log non è abilitata o se `loggingLevel` non è ERROR o INFO.

Identificatore: API_GW_EXECUTION_LOGGING_ENABLED

Tipi di risorse: AWS::ApiGateway::Stage, AWS::ApiGateway V2: :Stage

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

loggingLevel (opzionale), ▪Tipo: stringa, Impostazione predefinita: ERROR, INFO

Elenco separato da virgole dei livelli di registrazione di log specifici (ad esempio ERROR, INFO o ERROR,INFO).

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

api-gw-ssl-enabled

Verifica se una fase REST API utilizza un certificato SSL. La regola è NON_COMPLIANT se la fase REST API non ha un certificato SSL associato.

> **Note**
>
> Questa regola viene restituita `NOT_APPLICABLE` se l'GetIntegrationAPI restituisce `AWS` un tipo.

Identificatore: API_GW_SSL_ENABLED

Tipi di risorse: AWS::ApiGateway::Stage

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

CertificateIDs (opzionale), Tipo: CSV

Elenco separato da virgole degli ID di certificato client configurati in una fase REST API.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

api-gw-xray-enabled

Verifica se il tracciamento AWS X-Ray è abilitato sulle API REST di Amazon API Gateway. La regola è COMPLIANT se il tracciamento X-Ray è abilitato ed è NON_COMPLIANT in caso contrario.

Identificatore: API_GW_XRAY_ENABLED

Tipi di risorse: AWS::ApiGateway::Stage

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
   "TracingEnabled": BOOLEAN,
   "RestApiId": "my-rest-api-Id",
}
...
```

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

approved-amis-by-id

Verifica se le istanze EC2 in esecuzione utilizzano le Amazon Machine Image (AMI) specificate. Specifica un elenco di ID AMI approvati. Le istanze in esecuzione con le AMI non incluse in questo elenco sono NON_COMPLIANT.

Identificatore: APPROVED_AMIS_BY_ID

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

amiIds, Tipo: CSV

> Gli ID AMI (elenco separato da virgole di un massimo di 21 ID AMI o di 1024 caratteri in totale, a seconda di ciò che si verifica per primo).

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

approved-amis-by-tag

Verifica se le istanze in esecuzione utilizzano le Amazon Machine Image (AMI) specificate. Specifica i tag che identificano le AMI. Le istanze in esecuzione con le AMI che non hanno almeno uno dei tag specificati sono NON_COMPLIANT.

Identificatore: APPROVED_AMIS_BY_TAG

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Amis Value ByTag KeyAnd, Tipo: StringMap, Impostazione predefinita: tag-key:tag-value,other-tag-key

> Le AMI in base ai tag (elenco separato da virgole fino a 10; ad esempio `tag-key:tag-value`; ovvero `tag-key1` corrisponde alle AMI con `tag-key1`, `tag-key2:value2` corrisponde a `tag-key2` con value2).

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

appsync-associated-with-waf

Verifica se le AWS AppSync API sono associate agli elenchi di controllo degli accessi Web (ACL) AWS WAFv2. La regola è NON_COMPLIANT per un' AWS AppSync API se non è associata a un ACL web.

Identificatore: APPSYNC_ASSOCIATED_WITH_WAF

Tipi di AWS::AppSync::Graph risorse: QLaPi

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

WebAclARN waf (opzionale), Tipo: CSV

> Elenco separato da virgole dei nomi della risorsa Amazon (ARN) per le ACL Web autorizzate.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

appsync-authorization-check

Verifica se un' AWS AppSync API utilizza meccanismi di autorizzazione consentiti. La regola è NON_COMPLIANT se viene utilizzato un meccanismo di autorizzazione non approvato.

Identificatore: APPSYNC_AUTHORIZATION_CHECK

Tipi di risorse: AWS::AppSync::Graph QLaPi

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

AllowedAuthorizationTipi, Tipo: CSV

> Elenco separato da virgole dei meccanismi di autorizzazione consentiti AWS AppSync . I valori consentiti sono: "API_KEY", "AWS_LAMBDA", "AWS_IAM", "OPENID_CONNECT", "AMAZON_COGNITO_USER_POOLS".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

appsync-cache-encryption-at-rest

Verifica se una cache AWS AppSync API ha la crittografia a riposo abilitata. Questa regola è NON_COMPLIANT se " AtRest EncryptionEnabled è falso.

Identificatore: APPSYNC_CACHE_ENCRYPTION_AT_REST

Tipi di risorse: QLaPi AWS::AppSync::Graph

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

appsync-logging-enabled

Verifica se un'API ha la registrazione abilitata. AWS AppSync La regola è NON_COMPLIANT se la registrazione non è abilitata, oppure «field» non è né ERROR né ALLLogLevel.

Identificatore: APPSYNC_LOGGING_ENABLED

Tipi AWS::AppSync::Graph di risorse: QLaPi

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

fieldLoggingLevel (Facoltativo), Tipo: CSV

> Elenco separato da virgole dei livelli di registrazione di log di campi specifici (ad esempio ERROR, ALL).

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

athena-workgroup-encrypted-at-rest

Verifica se un gruppo di lavoro Amazon Athena è crittografato a riposo. La regola è NON_COMPLIANT se la crittografia dei dati a riposo non è abilitata per un gruppo di lavoro Athena.

Identificatore: ATHENA_WORKGROUP_ENCRYPTED_AT_REST

Tipi di risorse: AWS::Athena::WorkGroup

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

aurora-last-backup-recovery-point-created

Verifica se è stato creato un punto di ripristino per i cluster di database Amazon Aurora. La regola è NON_COMPLIANT se il cluster di database Amazon Relational Database Service (Amazon RDS) non dispone di un punto di ripristino corrispondente creato entro il periodo di tempo specificato.

Identificatore: AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▪Tipo: stringa

Tag dei cluster di database Aurora che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▪Tipo: stringa

ID del cluster di database Aurora che la regola deve verificare.

ripristino PointAgeValue (opzionale), Tipo: int, Impostazione predefinita: 1

Valore numerico per la durata massima consentita. Non superiore a 744 per le ore e 31 per i giorni.

ripristino PointAgeUnit (opzionale), ▪Tipo: stringa, Impostazione predefinita: giorni

Unità di tempo per la durata massima consentita. Valori accettati: "ore", "giorni".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

aurora-meets-restore-time-target

Verifica se il tempo di ripristino dei cluster Amazon Aurora DB soddisfa la durata specificata. La regola è NON_COMPLIANT se di LatestRestoreExecutionTimeMinutes un cluster Aurora DB è superiore a minuti. maxRestoreTime

Identificatore: AURORA_MEETS_RESTORE_TIME_TARGET

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Periodico

Regione AWS: AWS Tutte le regioni supportate

Parametri:

max RestoreTime, Tipo: int

Valore numerico per il runtime massimo di ripristino consentito.

resourceTags (opzionale), ▬Tipo: stringa

Tag dei cluster di database Aurora che la regola deve verificare, in formato JSON.

resourceId (opzionale), ▬Tipo: stringa

ID del cluster di database Aurora che la regola deve verificare.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

aurora-mysql-backtracking-enabled

Verifica se il backtrack è abilitato per un cluster MySQL di Amazon Aurora. La regola è NON_COMPLIANT se il backtrack non è abilitato per il cluster Aurora e se tale cluster utilizza MySQL.

Identificatore: AURORA_MYSQL_BACKTRACKING_ENABLED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Disponibile solo in Asia Pacifico (Mumbai), Europa (Parigi), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Europa (Londra), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Centrale), Cina (Ningxx) Ia), Regione Europa (Zurigo)

Parametri:

BacktrackWindowInHours (Opzionale), Tipo: doppio

Periodo di tempo in ore (fino a 72) per effettuare il backtrack del cluster MySQL Aurora.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

aurora-resources-protected-by-backup-plan

Verifica se i cluster di database Amazon Aurora sono protetti da un piano di backup. La regola è NON_COMPLIANT se il cluster di database Amazon Relational Database Service (Amazon RDS) non è protetto da un piano di backup.

Identificatore: AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▬Tipo: stringa

Tag dei cluster di database Aurora che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▬Tipo: stringa

ID del cluster di database Aurora che la regola deve verificare.

crossRegionList (Facoltativo), ▬Tipo: stringa

Elenco separato da virgole delle regioni di destinazione della copia di backup tra regioni da conservare

crossAccountList (Opzionale), ▬Tipo: stringa

Elenco separato da virgole degli account di destinazione della copia di backup tra account da conservare

maxRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione massimo in giorni per Vault Lock di Backup

minRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione minimo in giorni per Vault Lock di Backup

backup VaultLockCheck (opzionale), ▬Tipo: stringa

Valori accettati: "True" o "False". Immetti "True" per fare in modo che la regola verifichi se per la risorsa viene eseguito il backup in un vault bloccato

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

autoscaling-capacity-rebalancing

Verifica se il ribilanciamento della capacità è abilitato per i gruppi con dimensionamento automatico Amazon EC2 che utilizzano più tipi di istanze. La regola è NON_COMPLIANT se il ribilanciamento della capacità non è abilitato.

Identificatore: AUTOSCALING_CAPACITY_REBALANCING

Tipi di risorse: AWS::AutoScaling::AutoScaling Gruppo

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

autoscaling-group-elb-healthcheck-required

Verifica se i tuoi gruppi Amazon EC2 Auto Scaling associati a un Elastic Load Balancer utilizzano i controlli di integrità di Elastic Load Balancing. La regola è NON_COMPLIANT se i gruppi con dimensionamento automatico Amazon EC2 non utilizzano i controlli dell'integrità di Elastic Load Balancing.

Identificatore: AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

Tipi di risorse: gruppo AWS::AutoScaling::AutoScaling

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
   "LoadBalancerNames": "[my-load-balancer-1, my-load-balancer-2, my-load-
balancer-3, ...]",
   "HealthCheckType": HealthCheckType*"
}
...
```

*I valori validi sono `EC2` (impostazione predefinita), `ELB` e `VPC_LATTICE`. Il tipo di controllo dell'integrità `VPC_LATTICE` è riservato all'uso con VPC Lattice, un rilascio in anteprima soggetto a

modifiche. Per ulteriori informazioni, consulta Controlli dell'integrità per istanze Auto Scaling nella Guida per l'utente di Dimensionamento automatico Amazon EC2.

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

autoscaling-launchconfig-requires-imdsv2

Verifica se è abilitato solo IMDSv2. Questa regola è NON_COMPLIANT se la versione dei metadati non è inclusa nella configurazione di avvio o se entrambe le versioni V1 e V2 dei metadati sono abilitate.

Identificatore: AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2

Tipi di risorse: AWS::AutoScaling::LaunchConfiguration

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

autoscaling-launch-config-hop-limit

Verifica il numero di hop di rete che il token di metadati può percorrere. Questa regola è NON_COMPLIANT se il limite di hop di risposta dei metadati è maggiore di 1.

Identificatore: AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

Tipi di risorse: AWS::AutoScaling::LaunchConfiguration

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

autoscaling-launch-config-public-ip-disabled

Verifica se i gruppi con dimensionamento automatico Amazon EC2 hanno indirizzi IP pubblici abilitati tramite Configurazioni di avvio. La regola è NON_COMPLIANT se la configurazione di avvio per un gruppo Amazon EC2 Auto Scaling è impostata su «true». AssociatePublicIpAddress

Identificatore: AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

Tipi di risorse: AWS::AutoScaling::LaunchConfiguration

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

autoscaling-launch-template

Verifica se un gruppo con dimensionamento automatico Amazon Elastic Compute Cloud (EC2) è creato da un modello di avvio EC2. La regola è NON_COMPLIANT se il gruppo con dimensionamento non è creato da un modello di avvio EC2.

Identificatore: AUTOSCALING_LAUNCH_TEMPLATE

Tipi di risorse: AWS::AutoScaling::AutoScaling Gruppo

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

autoscaling-multiple-az

Verifica se il gruppo con dimensionamento automatico si estende su più zone di disponibilità. La regola è NON_COMPLIANT se il gruppo con dimensionamento automatico non si estende su più zone di disponibilità.

Identificatore: AUTOSCALING_MULTIPLE_AZ

Tipi di risorse: AWS::AutoScaling::AutoScaling Gruppo

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

minAvailabilityZones (Facoltativo), Tipo: int

Numero minimo di zone di disponibilità previste.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

autoscaling-multiple-instance-types

Verifica se un gruppo con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) utilizza più tipi di istanze. Questa regola è NON_COMPLIANT se il gruppo con dimensionamento automatico Amazon EC2 ha un solo tipo di istanza definito.

Identificatore: AUTOSCALING_MULTIPLE_INSTANCE_TYPES

Tipi di risorse: AWS::AutoScaling::AutoScaling Gruppo

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

backup-plan-min-frequency-and-min-retention-check

Verifica se un piano di backup dispone di una regola di backup che soddisfa la frequenza e il periodo di conservazione richiesti. La regola è NON_COMPLIANT se i punti di ripristino non vengono creati almeno con la stessa frequenza specificata o se scadono prima del periodo specificato.

Identificatore: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK

Tipi di risorse: AWS::Backup::BackupPlan

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

requiredFrequencyValue (Facoltativo), Tipo: int, Impostazione predefinita: 1

> Valore numerico per la frequenza di backup richiesta. Valore massimo di 24 per le ore e di 31 per i giorni.

requiredRetentionDays (Opzionale), Tipo: int, Impostazione predefinita: 35

Periodo di conservazione richiesto in giorni.

requiredFrequencyUnit (Opzionale), ▬Tipo: stringa, Impostazione predefinita: giorni

Unità di tempo per la frequenza di backup richiesta. Valori accettati: "ore", "giorni".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

backup-recovery-point-encrypted

Verifica se un punto di ripristino è crittografato. La regola è NON_COMPLIANT se il punto di ripristino non è crittografato.

Identificatore: BACKUP_RECOVERY_POINT_ENCRYPTED

Tipi di risorse: AWS::Backup::RecoveryPoint

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

backup-recovery-point-manual-deletion-disabled

Verifica se a un vault di backup è collegata una policy basata sulle risorse che impedisce l'eliminazione dei punti di ripristino. La regola è NON_COMPLIANT se Backup Vault non dispone di policy basate sulle risorse o ha policy prive di un'istruzione 'Deny' adeguata (istruzione con

backup: DeleteRecovery Point, backup: e backup: permissions). UpdateRecovery PointLifecycle PutBackupVaultAccessPolicy

Identificatore: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED

Tipi di risorse: AWS::Backup::BackupVault

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

principalArnList (Facoltativo), Tipo: CSV

Elenco separato da virgole di Amazon Resource Names (ARN) di AWS Identity and Access Management (IAM) per la regola da NON controllare.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

backup-recovery-point-minimum-retention-check

Verifica se un punto di ripristino scade non prima del periodo specificato. La regola è NON_COMPLIANT se il punto di ripristino ha un punto di conservazione inferiore al periodo di conservazione richiesto.

Identificatore: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK

Tipi di risorse: AWS::Backup::RecoveryPoint

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

requiredRetentionDays (Facoltativo), Tipo: int, Impostazione predefinita: 35

Periodo di conservazione richiesto in giorni.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

beanstalk-enhanced-health-reporting-enabled

Verifica se un ambiente AWS Elastic Beanstalk è configurato per un reporting sanitario avanzato. La regola è COMPLIANT se l'ambiente è configurato per la creazione di report sull'integrità avanzati. La regola è NON_COMPLIANT se l'ambiente è configurato per la creazione di report sull'integrità di base.

Identificatore: BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED

Tipi di risorse: AWS::ElasticBeanstalk::Environment

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

clb-desync-mode-check

Verifica se i Classic Load Balancer (CLB) sono configurati con una modalità di mitigazione desincronizzata definita dall'utente. La regola è NON_COMPLIANT se la modalità di mitigazione desincronizzata del CLB non corrisponde alla modalità di mitigazione desincronizzata definita dall'utente.

Identificatore: CLB_DESYNC_MODE_CHECK

Tipi di risorse: AWS::ElasticLoadBalancing::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

desyncMode, Tipo: CSV

Elenco di valori separati da virgole. Puoi selezionare un massimo di due valori. I valori validi includono "Defensive", "Strictest" e "Monitor".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

clb-multiple-az

Verifica se un Classic Load Balancer si estende su più zone di disponibilità (AZ). La regola è NON_COMPLIANT se un Classic Load Balancer si estende su meno di due zone di disponibilità o se non copre il numero di zone di disponibilità menzionato nel parametro `minAvailabilityZones` (se fornito).

Identificatore: CLB_MULTIPLE_AZ

Tipi di risorse: AWS::ElasticLoadBalancing::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

minAvailabilityZones (Facoltativo), Tipo: int

Numero minimo desiderato di zone di disponibilità previste. I valori validi sono compresi tra 2 e 10 (inclusi). Se non viene specificato alcun valore per il parametro, il valore predefinito è 2.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudformation-stack-drift-detection-check

Verifica se la configurazione effettiva di uno stack AWS CloudFormation (AWS CloudFormation) è diversa, o si è allontanata, dalla configurazione prevista. Uno stack è considerato come deviato se una o più delle relative risorse risultano diverse dalla configurazione attesa. La regola e lo stack sono COMPLIANT quando lo stato di deviazione di stack è IN_SYNC. La regola è NON_COMPLIANT se lo stato di deviazione dello stack è DRIFTED.

> **Note**
>
> Questa regola esegue l' DetectStackDrift operazione su ogni stack del tuo account. L' DetectStackDrift operazione può richiedere fino a diversi minuti, a seconda del numero di risorse contenute nello stack. Dato che il tempo massimo di esecuzione di questa regola è limitato a 15 minuti, è possibile che la regola scada prima di completare la valutazione di tutti gli stack nell'account.
> Se si verifica questo problema, consigliamo di limitare il numero di stack nell'ambito della regola utilizzando i tag. Puoi eseguire le operazioni indicate di seguito:
>
> 1. Dividi gli stack in gruppi, ognuno con un tag diverso.
> 2. Applica lo stesso tag a tutti gli stack di quel gruppo.
> 3. Inserisci più istanze di questa regola nell'account, ognuna definita da un tag diverso. Ciò consente a ciascuna istanza della regola di elaborare solo gli stack con il tag corrispondente menzionato nel proprio ambito.

Identifier (Identificatore): CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

Tipi di risorse: AWS::CloudFormation::Stack

Tipo di trigger: Modifiche alla configurazione e periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

formazione di nuvole RoleArn, ▪Tipo: stringa

Amazon Resource Name (ARN) del ruolo IAM con autorizzazioni di policy per rilevare la deriva degli stack. AWS CloudFormation Per informazioni sulle autorizzazioni IAM richieste per il ruolo,

consulta Rilevamento delle modifiche di configurazione non gestite agli stack e alle risorse | Considerazioni sulla rilevazione della deriva nella Guida per l'utente. AWS CloudFormation

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudformation-stack-notification-check

Verifica se i tuoi CloudFormation stack inviano notifiche di eventi a un argomento di Amazon SNS. Facoltativamente, verifica se vengono usati gli argomenti Amazon SNS specificati. La regola è NON_COMPLIANT se CloudFormation gli stack non inviano notifiche.

Identificatore: CLOUDFORMATION_STACK_NOTIFICATION_CHECK

Tipi di risorse: AWS::CloudFormation::Stack

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Disponibile solo in Cina (Pechino), Asia Pacifico (Mumbai), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Europa (Londra), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Regione Centrale), Cina (Ningxia)

Parametri:

snsTopic1 (opzionale), ▪Tipo: stringa

ARN dell'argomento SNS.

snsTopic2 (opzionale), ▪Tipo: stringa

ARN dell'argomento SNS.

snsTopic3 (opzionale), ▪Tipo: stringa

ARN dell'argomento SNS.

snsTopic4 (opzionale), ▪Tipo: stringa

ARN dell'argomento SNS.

snsTopic5 (opzionale), ▪Tipo: stringa

ARN dell'argomento SNS.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudfront-accesslogs-enabled

Verifica se CloudFront le distribuzioni Amazon sono configurate per fornire log di accesso a un bucket Amazon S3. La regola è NON_COMPLIANT se una distribuzione non ha configurato la registrazione. CloudFront

Identificatore: CLOUDFRONT_ACCESSLOGS_ENABLED

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

S3 BucketName (opzionale), ▪Tipo: stringa

Il nome del bucket Amazon S3 per l'archiviazione dei log di accesso al server.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudfront-associated-with-waf

Verifica se CloudFront le distribuzioni Amazon sono associate a Web Application Firewall (WAF) o WAFv2 Web Access Control List (ACL). La regola è NON_COMPLIANT se una distribuzione non è associata a un CloudFront ACL web WAF.

Identificatore: CLOUDFRONT_ASSOCIATED_WITH_WAF

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

waf WebAclIds (opzionale), Tipo: CSV

> Elenco separato da virgole degli ID dell'ACL Web per WAF o dei nomi della risorsa Amazon (ARN) dell'ACL Web per WAFV2.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudfront-custom-ssl-certificate

Verifica se il certificato associato a una CloudFront distribuzione Amazon è il certificato SSL predefinito. La regola è NON_COMPLIANT se una CloudFront distribuzione utilizza il certificato SSL predefinito.

Identificatore: CLOUDFRONT_CUSTOM_SSL_CERTIFICATE

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudfront-default-root-object-configured

Verifica se una CloudFront distribuzione Amazon è configurata per restituire un oggetto specifico che è l'oggetto root predefinito. La regola è NON_COMPLIANT se la distribuzione CloudFront Amazon non ha un oggetto root predefinito configurato.

Identificatore: CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

cloudfront-no-deprecated-ssl-protocols

Verifica se CloudFront le distribuzioni utilizzano protocolli SSL obsoleti per la comunicazione HTTPS tra edge location e origini personalizzate. CloudFront Questa regola è NON_COMPLIANT per una distribuzione se alcuni 'protocolli' includono 'SSLv3'. CloudFront OriginSsl

Identificatore: CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudfront-origin-access-identity-enabled

Verifica se CloudFront la distribuzione con il tipo Amazon S3 Origin ha configurato l'identità di accesso all'origine. La regola è NON_COMPLIANT se la CloudFront distribuzione è supportata da S3 e qualsiasi tipo di origine non è configurato con OAI o se l'origine non è un bucket S3.

> **Note**
>
> La regola non restituisce il risultato NOT_APPLICABLE se l'origine non è un bucket S3.

Identificatore: CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudfront-origin-failover-enabled

Verifica se un gruppo di origine è configurato per la distribuzione di almeno due origini nel gruppo di origine per Amazon CloudFront. La regola è NON_COMPLIANT se non ci sono gruppi di origine per la distribuzione.

Identificatore: CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudfront-s3-origin-access-control-enabled

Verifica se una CloudFront distribuzione Amazon con un tipo Amazon Simple Storage Service (Amazon S3) Origin ha il controllo dell'accesso all'origine (OAC) abilitato. La regola è NON_COMPLIANT per le distribuzioni CloudFront con origini Amazon S3 che non hanno OAC abilitato.

Identificatore: CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudfront-s3-origin-non-existent-bucket

Verifica se CloudFront le distribuzioni Amazon puntano a un bucket S3 inesistente. La regola è NON_COMPLIANT se `S3 `per una distribuzione punta a un bucket S3 OriginConfig inesistente. CloudFront La regola non valuta i bucket S3 con hosting di siti Web statici.

Identificatore: CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Periodico

Regione AWS: disponibile solo nelle regioni Cina (Pechino), Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudfront-security-policy-check

Verifica se CloudFront le distribuzioni Amazon utilizzano una politica di sicurezza minima e una suite di crittografia TLSv1.2 o superiore per le connessioni dei visualizzatori. Questa regola è NON_COMPLIANT per una distribuzione se è inferiore a TLSv1.2_2018. CloudFront minimumProtocolVersion

Identificatore: CLOUDFRONT_SECURITY_POLICY_CHECK

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudfront-sni-enabled

Verifica se CloudFront le distribuzioni Amazon utilizzano un certificato SSL personalizzato e sono configurate per utilizzare SNI per soddisfare le richieste HTTPS. La regola è NON_COMPLIANT se è associato un certificato SSL personalizzato, ma il metodo di supporto SSL è un indirizzo IP dedicato.

Identificatore: CLOUDFRONT_SNI_ENABLED

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

cloudfront-traffic-to-origin-encrypted

Verifica se CloudFront le distribuzioni Amazon stanno crittografando il traffico verso origini personalizzate. La regola è NON_COMPLIANT se «OriginProtocolPolicy» è «solo http» o se «Policy» è «match-viewer» e «OriginProtocolPolicy» è «allow-all». ViewerProtocol

Identificatore: CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudfront-viewer-policy-https

Verifica se le tue CloudFront distribuzioni Amazon utilizzano HTTPS (direttamente o tramite un reindirizzamento). La regola è NON_COMPLIANT se il valore di ViewerProtocolPolicy è impostato su 'allow-all' per o per. DefaultCacheBehavior CacheBehaviors

Identificatore: CLOUDFRONT_VIEWER_POLICY_HTTPS

Tipi di risorse: AWS::CloudFront::Distribution

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudtrail-all-read-s3-data-event-check

Verifica se un trail AWS CloudTrail multiregionale è abilitato e registra tutti gli eventi di lettura dei dati S3 relativi ai tuoi bucket. La regola è NON_COMPLIANT se nessun trail multiregione registra tutti i tipi di eventi di dati S3 letti per tutti i bucket S3 attuali e futuri.

Identificatore: CLOUDTRAIL_ALL_READ_S3_DATA_EVENT_CHECK

Tipi di risorse: AWS::::Account

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudtrail-all-write-s3-data-event-check

Verifica se un trail AWS CloudTrail multiregionale è abilitato e registra tutti gli eventi di scrittura dei dati S3 per i tuoi bucket. La regola è NON_COMPLIANT se nessun trail log multiregione registra tutti i tipi di eventi di dati S3 di scrittura per tutti i bucket S3 attuali e futuri.

Identificatore: CLOUDTRAIL_ALL_WRITE_S3_DATA_EVENT_CHECK

Tipi di risorse: AWS::::Account

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

registrazione degli accessi a cloudtrail-s3-bucket

Verifica se le configurazioni dei bucket S3 per i tuoi AWS CloudTrail log hanno abilitato la registrazione degli accessi al server Amazon S3. La regola è NON_COMPLIANT se almeno un bucket S3 per un trail non ha la registrazione degli accessi al server S3 abilitata. CloudTrail

Identificatore: CLOUDTRAIL_S3_BUCKET_ACCESS_LOGGING

Tipi di risorse: AWS::CloudTrail::Trail

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudtrail-s3-bucket-accesso pubblico vietato

Verifica se le configurazioni del bucket S3 per i tuoi log bloccano l'accesso pubblico. AWS CloudTrail La regola è NON_COMPLIANT se almeno un bucket S3 per un trail è accessibile pubblicamente. CloudTrail

Identificatore: CLOUDTRAIL_S3_BUCKET_PUBLIC_ACCESS_PROIBITED

Tipi di risorse: AWS::CloudTrail::Trail

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudtrail-s3-dataevents-enabled

Verifica se almeno un AWS CloudTrail trail registra gli eventi relativi ai dati di Amazon Simple Storage Service (Amazon S3) per tutti i bucket S3. La regola è NON_COMPLIANT se sono presenti trail o se nessun trail registra gli eventi di dati S3.

Identificatore: CLOUDTRAIL_S3_DATAEVENTS_ENABLED

Tipo di trigger: Periodico

Regione AWS: tutte le regioni supportate AWS

Parametri:

S3 BucketNames (opzionale), ▬Tipo: stringa

Elenco separato da virgole dei nomi di bucket S3 per i quali deve essere abilitata la registrazione di log degli eventi di dati. Controlli di comportamento predefiniti per tutti i bucket S3.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudtrail-security-trail-enabled

Verifica che esista almeno un AWS CloudTrail percorso definito con le migliori pratiche di sicurezza. Questa regola è COMPLIANT se esiste almeno un trail che soddisfa tutti i seguenti requisiti:

- registra gli eventi dei servizi globali
- è un trail multi-regione
- dispone della convalida dei file di log abilitata
- è crittografato con una chiave KMS
- registra gli eventi relativi a letture e scritture
- registra gli eventi di gestione dei record
- non esclude alcun evento di gestione

Questa regola è NON_COMPLIANT se nessun trail soddisfa tutti i criteri sopra menzionati.

Identificatore: CLOUDTRAIL_SECURITY_TRAIL_ENABLED

Tipo di trigger: Periodico

Regione AWS: tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

cloudwatch-alarm-action-check

Verifica se gli CloudWatch allarmi hanno un'azione configurata per lo stato ALARM, INSUFFICIENT_DATA o OK. Facoltativamente, controlla se le azioni corrispondono a un ARN indicato. La regola è NON_COMPLIANT se non è stata specificata alcuna azione per l'allarme o per il parametro opzionale.

Identificatore: CLOUDWATCH_ALARM_ACTION_CHECK

Tipi di risorse: AWS::CloudWatch::Alarm

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

allarme ActionRequired, ▪Tipo: stringa, Impostazione predefinita: true

Gli allarmi hanno almeno un'operazione.

insufficiente DataAction Richiesto, ▪Tipo: stringa, Impostazione predefinita: true

Gli allarmi hanno almeno un'azione quando l'allarme passa allo stato INSUFFICIENT_DATA da qualsiasi altro stato.

ok ActionRequired, ▪Tipo: stringa, Impostazione predefinita: false

Gli allarmi hanno almeno un'azione quando l'allarme passa allo stato OK da qualsiasi altro stato.

action1 (opzionale), ▪Tipo: stringa

Operazione da eseguire, specificata come ARN.

action2 (opzionale), ▪Tipo: stringa

Operazione da eseguire, specificata come ARN.

action3 (opzionale), ▪Tipo: stringa

Operazione da eseguire, specificata come ARN.

action4 (opzionale), ▪Tipo: stringa

Operazione da eseguire, specificata come ARN.

action5 (opzionale), ▪Tipo: stringa

Operazione da eseguire, specificata come ARN.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudwatch-alarm-action-enabled-check

Verifica se CloudWatch le azioni di Amazon Alarm sono abilitate. La regola è NON_COMPLIANT se CloudWatch le azioni degli allarmi non sono abilitate.

Identificatore: CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

Tipi di risorse: AWS::CloudWatch::Alarm

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudwatch-alarm-resource-check

Verifica se un tipo di risorsa ha un CloudWatch allarme per la metrica indicata. Come tipo di risorsa, puoi specificare volumi EBS, istanze EC2, cluster Amazon RDS o bucket S3. La regola è CONFORME se la metrica indicata ha un ID di risorsa e un allarme. CloudWatch

Identificatore: CLOUDWATCH_ALARM_RESOURCE_CHECK

Tipi di risorse:,, AWS::EC2::Instance AWS::RDS::DBCluster, AWS::S3::Bucket AWS::EC2::Volume

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceType, ▬Tipo: stringa

AWS tipo di risorsa. Il valore può essere uno dei seguenti: AWS::EC2::Volume, AWS::EC2::Instance, AWS::RDS::DBCluster, or AWS::S3::Bucket.

metricName, ▬Tipo: stringa

Il nome della metrica associata all'allarme (ad esempio "CPUUtilization" per le istanze EC2).

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

cloudwatch-alarm-settings-check

Verifica se gli CloudWatch allarmi con il nome della metrica specificato hanno le impostazioni specificate.

Identificatore: CLOUDWATCH_ALARM_SETTINGS_CHECK

Tipi di risorse: AWS::CloudWatch::Alarm

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

metricName, ▬Tipo: stringa

Nome del parametro associato all'allarme.

threshold (opzionale), Tipo: int

Il valore rispetto al quale viene paragonata la statistica specificata.

evaluationPeriods (opzionale), Tipo: int

Il numero di periodi in cui i dati vengono paragonati alla soglia specificata.

period (opzionale), Tipo: int, Impostazione predefinita: 300

Periodo, in secondi, durante il quale viene applicata la statistica specificata.

comparisonOperator (opzionale), ▬Tipo: stringa

L'operazione per confrontare la statistica e la soglia specificate (ad esempio, 'GreaterThanThreshold').

statistic (opzionale), ▬Tipo: stringa

La statistica per la metrica associata all'allarme (ad esempio "Average" o "Sum").

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloudwatch-log-group-encrypted

Verifica se Amazon CloudWatch Log Groups sono crittografati con una chiave AWS KMS o un ID chiave AWS KMS specificato. La regola è NON_COMPLIANT se un gruppo di CloudWatch log non è crittografato con una chiave KMS o è crittografato con una chiave KMS non fornita nel parametro della regola.

Identificatore: CLOUDWATCH_LOG_GROUP_ENCRYPTED

Tipi di risorse: AWS::Logs::LogGroup

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

KmsKeyId (Facoltativo), ▬Tipo: stringa

Nome della risorsa Amazon (ARN) dell'ID della chiave KMS utilizzata per crittografare il gruppo di log.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloud-trail-cloud-watch-logs-enabled

Verifica se i AWS CloudTrail trail sono configurati per inviare log a log. CloudWatch Il percorso è NON_COMPLIANT se la CloudWatchLogsLogGroupArn proprietà del percorso è vuota.

Identifier (Identificatore): CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

Tipi di risorse: AWS::CloudTrail::Trail

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

previsto DeliveryWindowAge (opzionale), Tipo: int

Età massima, espressa in ore, dell'ultima consegna CloudWatch dei registri conformi.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

cloudtrail-enabled

> **Important**
>
> Per questa regola, l'identificatore (CLOUD_TRAIL_ENABLED) e il nome della regola (cloudtrail-enabled) sono diversi.

Verifica se un AWS CloudTrail trail è abilitato nel tuo account. AWS La regola è NON_COMPLIANT se un trail non è abilitato. Facoltativamente, la regola controlla uno specifico bucket S3, un argomento di Amazon Simple Notification Service (Amazon SNS) e un gruppo di log. CloudWatch

Identificatore: CLOUD_TRAIL_ENABLED

Tipo di trigger: Periodico

Regione AWS: tutte le regioni supportate AWS

Parametri:

s3 BucketName (opzionale), ▪Tipo: stringa

Nome del bucket S3 a cui CloudTrail inviare i file di registro.

snsTopicArn (Facoltativo), ▪Tipo: stringa

Argomento SNS ARN da utilizzare CloudTrail per le notifiche.

cloud WatchLogsLogGroupArn (opzionale), ▪Tipo: stringa

CloudWatch ARN del gruppo di log a CloudTrail cui inviare dati.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloud-trail-encryption-enabled

Verifica se AWS CloudTrail è configurato per utilizzare la crittografia lato server (SSE) AWS Key Management Service (AWS KMS). La regola è CONFORME se è definita. KmsKeyId

Identifier (Identificatore): CLOUD_TRAIL_ENCRYPTION_ENABLED

Tipi di risorse: AWS::CloudTrail::Trail

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cloud-trail-log-file-validation-enabled

Verifica se AWS CloudTrail crea un file digest firmato con log. AWS raccomanda che la convalida del file sia abilitata su tutti i percorsi. La regola è NON_COMPLIANT se la convalida non è abilitata.

Identifier (Identificatore): CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

Tipi di risorse: AWS::CloudTrail::Trail

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cmk-backing-key-rotation-enabled

Verifica se la rotazione automatica delle chiavi è abilitata per ogni chiave e corrisponde all'ID chiave della chiave KMS creata dal cliente. AWS La regola è NON_COMPLIANT se il ruolo del registratore AWS Config per una risorsa non dispone dell'autorizzazione kms:. DescribeKey

> **Note**
>
> La rotazione automatica delle chiavi non è supportata per le chiavi KMS asimmetriche, le chiavi KMS HMAC, le chiavi KMS con materiale della chiave importato o le chiavi KSM negli archivi delle chiavi personalizzate.

Identifier (Identificatore): CMK_BACKING_KEY_ROTATION_ENABLED

Tipi di risorse: AWS::KMS::Key

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

codebuild-project-artifact-encryption

Verifica se un AWS CodeBuild progetto ha la crittografia abilitata per tutti i suoi artefatti. La regola è NON_COMPLIANT se "encryptionDisabled" è impostato su "true" per qualsiasi configurazione di artefatto primario o secondario (se presente).

Identificatore: CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION

Tipi di risorse: AWS::CodeBuild::Project

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

codebuild-project-environment-privileged-check

Verifica se un ambiente di progetto ha la modalità privilegiata abilitata. AWS CodeBuild La regola è NON_COMPLIANT per un progetto CodeBuild se 'PrivilegedMode' è impostato su 'true'.

Identificatore: CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

Tipi di risorse: AWS::CodeBuild::Project

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

exemptedProjects (opzionale), Tipo: CSV

Elenco separato da virgole di nomi di CodeBuild progetto che possono avere 'PrivilegedMode' con valore 'true'.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

codebuild-project-envvar-awscred-check

Verifica se il progetto contiene le variabili di ambiente _ACCESS_KEY_ID e _SECRET_ACCESS_KEY. AWS AWS La regola è NON_COMPLIANT quando le variabili di ambiente del progetto contengono credenziali in testo normale.

Identificatore: CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK

Tipi di risorse: AWS::CodeBuild::Project

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

codebuild-project-logging-enabled

Verifica se un ambiente di AWS CodeBuild progetto ha almeno un'opzione di registro abilitata. La regola è NON_COMPLIANT se lo stato di tutte le configurazioni di log attuali è impostato su "DISABLED".

Identificatore: CODEBUILD_PROJECT_LOGGING_ENABLED

Tipi di risorse: AWS::CodeBuild::Project

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

s3 BucketNames (opzionale), ➖Tipo: stringa

Elenco separato da virgole dei nomi di bucket Amazon S3 a cui inviare i log se i log S3 sono configurati.

cloud WatchGroupNames (opzionale), ➖Tipo: stringa

Elenco separato da virgole dei nomi dei gruppi di CloudWatch log di Amazon a cui devono essere inviati i log se CloudWatch i log sono configurati.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

codebuild-project-s3-logs-encrypted

Verifica se un AWS CodeBuild progetto configurato con Amazon S3 Logs ha la crittografia abilitata per i log. La regola è NON_COMPLIANT se 'EncryptionDisabled' è impostato su 'true' in un S3 di un progetto. LogsConfig CodeBuild

Identificatore: CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

Tipi di risorse: AWS::CodeBuild::Project

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

exemptedProjects (opzionale), Tipo: CSV

Elenco separato da virgole di nomi di CodeBuild progetto a cui è consentito generare registri non crittografati.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

codebuild-project-source-repo-url-check

Verifica se l'URL del repository di origine Bitbucket contiene o meno le credenziali di accesso. La regola è NON_COMPLIANT se l'URL contiene le informazioni di accesso e COMPLIANT in caso contrario.

Identificatore: CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

Tipi di risorse: AWS::CodeBuild::Project

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

codedeploy-auto-rollback-monitor-enabled

Verifica se il gruppo di istanze implementate è configurato con il rollback automatico dell'implementazione e il monitoraggio dell'implementazione con allarmi collegati. La regola è NON_COMPLIANT se AutoRollbackConfiguration o non è AlarmConfiguration stata configurata o non è abilitata.

Identificatore: CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED

Tipi di risorse: AWS::CodeDeploy::DeploymentGroup

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

codedeploy-ec2-minimum-healthy-hosts-configured

Verifica se il gruppo di istanze implementate per la piattaforma di calcolo EC2/on-premise è configurato con una percentuale minima del parco istanze di host integri o con un numero di host superiore o uguale alla soglia di input. La regola è NON_COMPLIANT se uno dei due valori è inferiore alla soglia.

Identificatore: CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED

Tipi di risorse: AWS::CodeDeploy::DeploymentGroup

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

minimo HealthyHostsFleetPercent (opzionale), Tipo: int, Impostazione predefinita: 66

Percentuale minima del parco istanze di host integri durante l'implementazione. Il valore predefinito è il 66 percento.

minimo HealthyHostsHostCount (opzionale), Tipo: int, Impostazione predefinita: 1

Numero minimo di host integri nel parco istanze durante l'implementazione. Il valore predefinito è impostato su 1.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

codedeploy-lambda-allatonce-traffic-shift-disabled

Verifica se il gruppo di istanze implementate per la piattaforma di calcolo Lambda non utilizza la configurazione di implementazione predefinita. La regola è NON_COMPLIANT se il gruppo di distribuzione utilizza la configurazione di distribuzione 'Predefinita. CodeDeploy LambdaAllAtOnce'.

Identificatore: CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED

Tipi di risorse: AWS::CodeDeploy::DeploymentGroup

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

codepipeline-deployment-count-check

Verifica se la prima fase di distribuzione AWS CodePipeline esegue più di una distribuzione. Facoltativamente, verifica se ciascuna delle fasi successive rimanenti effettua l'implementazione su un numero di implementazioni superiore a quello specificato (`deploymentLimit`).

Identifier (Identificatore): CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

Tipi di risorse: AWS::CodePipeline::Pipeline

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile soltanto nelle regioni Asia Pacifico (Mumbai), Europa (Parigi), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Europa (Londra), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Centrale)

Parametri:

deploymentLimit (opzionale), Tipo: int

Il numero massimo di distribuzioni che ciascuna fase può eseguire.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

codepipeline-region-fanout-check

Verifica se ogni fase della fase si AWS CodePipeline schiera a più di N volte il numero delle regioni dispiegate in tutte le fasi combinate precedenti, dove N è il numero di fanout della regione. AWS CodePipeline La prima fase di implementazione è in grado di distribuire a un massimo di una regione, mentre la seconda fase di implementazione è in grado di distribuire a un numero massimo specificato nel `regionFanoutFactor`. Se non si fornisce una `regionFanoutFactor`, per impostazione predefinita il valore è tre. Ad esempio: se la prima fase di distribuzione è rivolta a una regione e la seconda fase di distribuzione è rivolta a tre regioni, la terza fase di distribuzione è in grado di distribuire a 12 regioni, ovvero, alla somma delle fasi precedenti moltiplicata per il numero (tre) di fan-out della regione. La regola è NON_COMPLIANT se la distribuzione è in più di una regione nella prima fase o in tre regioni nella seconda fase o in 12 regioni nella terza fase.

Identifier (Identificatore): CODEPIPELINE_REGION_FANOUT_CHECK

Tipi di risorse: AWS::CodePipeline::Pipeline

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile soltanto nelle regioni Asia Pacifico (Mumbai), Europa (Parigi), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Europa (Londra), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Centrale)

Parametri:

regionFanoutFactor (Facoltativo), Tipo: int, Impostazione predefinita: 3

Il numero di regioni in cui si AWS CodePipeline è schierato in tutte le fasi precedenti è il numero accettabile di regioni in cui ogni fase può schierarsi.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

custom-eventbus-policy-attached

Verifica se agli Amazon EventBridge Custom Event Bus è associata una policy basata sulle risorse. La regola è NON_COMPLIANT se a una policy del router di eventi personalizzata non è collegata una policy basata sulle risorse.

Identificatore: CUSTOM_EVENTBUS_POLICY_ATTACHED

Tipi di risorse: AWS::Events::EventBus

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

custom-schema-registry-policy-attached

Verifica se ai registri EventBridge dello schema Amazon personalizzati è associata una politica delle risorse. La regola è NON_COMPLIANT per i registri dello schema personalizzati senza una policy basata sulle risorse collegata.

Identificatore: CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED

Tipi di risorse: AWS::EventSchemas::Registry

Tipo di trigger: Periodico

Regione AWS: Disponibile solo in Europa (Stoccolma), Asia Pacifico (Mumbai), Europa (Parigi), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Asia Pacifico (Hong Kong), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Europa (Londra), Asia

Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), Asia Regione del Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Centrale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

cw-loggroup-retention-period-check

Verifica se un periodo di CloudWatch LogGroup conservazione di Amazon è impostato su più di 365 giorni oppure se è impostato un periodo di conservazione specificato. La regola è NON_COMPLIANT se il periodo di conservazione è inferiore`MinRetentionTime`, se specificato, a 365 giorni.

> **Note**
>
> Se l'impostazione di conservazione è "Nessuna scadenza" per un gruppo di log, la regola viene contrassegnata come COMPLIANT.

Identificatore: CW_LOGGROUP_RETENTION_PERIOD_CHECK

Tipi di risorse: AWS::Logs::LogGroup

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

LogGroupNames (Facoltativo), Tipo: CSV

Un elenco separato da virgole dei nomi dei gruppi di log per verificare il periodo di conservazione.

MinRetentionTime (Opzionale), Tipo: int

Specifica il tempo di conservazione. I valori validi sono: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827 e 3653. Il periodo di conservazione predefinito è 365 giorni.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dax-encryption-enabled

Verifica se i cluster Acceleratore Amazon DynamoDB (DAX) sono crittografati. La regola è NON_COMPLIANT se un cluster DAX non è crittografato.

Identificatore: DAX_ENCRYPTION_ENABLED

Tipi di risorse: AWS::DAX::Cluster

Tipo di trigger: Periodico

Regione AWS: disponibile soltanto nelle regioni Asia Pacifico (Mumbai), Europa (Parigi), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Europa (Londra), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), Asia Pacifico (Singapore), Asia Pacifico (Sydney)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

crittografia dax-tls-endpoint

Verifica se il cluster Amazon DynamoDB Accelerator (DAX) è impostato su TLS. ClusterEndpointEncryptionType La regola è NON_COMPLIANT se un cluster DAX non è crittografato da Transport Layer Security (TLS).

Identificatore: DAX_TLS_ENDPOINT_ENCRYPTION

Tipi di risorse: AWS::DAX::Cluster

Tipo di trigger: Periodico

Regione AWS: disponibile soltanto nelle regioni Asia Pacifico (Mumbai), Europa (Parigi), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Europa (Londra), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), Asia Pacifico (Singapore), Asia Pacifico (Sydney)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

db-instance-backup-enabled

Verifica se per le istanze database RDS sono abilitati i backup. Facoltativamente, la regola verifica il periodo di retention dei backup e la finestra di backup.

Identificatore: DB_INSTANCE_BACKUP_ENABLED

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

backupRetentionPeriod (Facoltativo), Tipo: int

Periodo di conservazione per i backup.

backupRetentionMinimum (Opzionale), Tipo: int

Periodo di conservazione minimo per i backup.

preferredBackupWindow (Opzionale), ➖Tipo: stringa

Intervallo di tempo in cui vengono creati backup.

checkReadReplicas (Opzionale), Tipo: booleano

Verifica se per le istanze database RDS sono abilitati backup per le repliche di lettura.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

desired-instance-tenancy

Verifica la presenza di un valore "tenancy" nelle istanze EC2. Verifica inoltre se gli ID AMI sono specificati per l'avvio da tali AMI o se gli ID host vengono avviati su tali host dedicati. La regola è COMPLIANT se l'istanza corrisponde a un host e a un'AMI, se specificata, in un elenco.

Identificatore: DESIRED_INSTANCE_TENANCY

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

tenancy, ▪Tipo: stringa

La tenancy desiderata delle istanze. I valori validi sono DEDICATED, HOST e DEFAULT.

imageId (opzionale), Tipo: CSV

La regola valuta le istanze avviate solo dalle AMI con gli ID specificati. Separa più ID AMI con virgole.

hostId (opzionale), Tipo: CSV

Gli ID degli host dedicati di EC2 in cui verranno avviate le istanze. Separa più ID host con virgole.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

desired-instance-type

Verifica se le istanze EC2 sono del tipo specificato. La regola è NON_COMPLIANT se un'istanza EC2 non è specificata nell'elenco dei parametri. Per un elenco dei tipi di istanza EC2 supportati, consulta Tipi di istanza nella Guida per l'utente di EC2 per le istanze Linux.

Identificatore: DESIRED_INSTANCE_TYPE

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

instanceType, Tipo: CSV

Elenco di tipi di istanza EC2 separati da virgole (ad esempio, "t2.small, m4.large, i2.xlarge").

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dms-auto-minor-version-upgrade-check

Verifica se in un'istanza di replica del AWS Database Migration Service (AWS DMS) sono abilitati gli aggiornamenti automatici delle versioni secondarie. La regola è NON_COMPLIANT se un'istanza di replica AWS DMS non è configurata con aggiornamenti automatici delle versioni secondarie.

Identificatore: DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

Tipi di risorse: AWS::DMS::ReplicationInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dms-endpoint-ssl-configured

Verifica se gli endpoint del AWS Database Migration Service (AWS DMS) sono configurati con una connessione SSL. La regola è NON_COMPLIANT se AWS DMS non dispone di una connessione SSL configurata.

Identificatore: DMS_ENDPOINT_SSL_CONFIGURED

Tipi di risorse: AWS::DMS::Endpoint

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

autenticazione dms-mongo-db abilitata

Verifica se gli endpoint AWS del Database Migration Service (AWS DMS) per gli archivi MongoDb dati sono abilitati per l'autenticazione basata su password e il controllo degli accessi. La regola è NON_COMPLIANT se l'autenticazione basata su password e il controllo degli accessi non sono abilitati.

Identificatore: DMS_MONGO_DB_AUTHENTICATION_ENABLED

Tipi di risorse: AWS::DMS::Endpoint

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dms-neptune-iam-abilitato all'autorizzazione

Verifica se un endpoint AWS Database Migration Service (AWS DMS) per i database Amazon Neptune è configurato con l'autorizzazione IAM. La regola è NON_COMPLIANT se un endpoint AWS DMS in cui Neptune è l'obiettivo è impostato su false. IamAuthEnabled

Identificatore: DMS_NEPTUNE_IAM_AUTHORIZATION_ENABLED

Tipi di risorse: AWS::DMS::Endpoint

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

abilitato per dms-redis-tls

Verifica se gli endpoint AWS Database Migration Service (AWS DMS) per gli archivi dati Redis sono abilitati per la crittografia TLS/SSL dei dati comunicati con altri endpoint. La regola è NON_COMPLIANT se la crittografia TLS/SSL non è abilitata.

Identificatore: DMS_REDIS_TLS_ENABLED

Tipi di risorse: AWS::DMS::Endpoint

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dms-replication-not-public

Verifica se le istanze di replica del AWS Database Migration Service (AWS DMS) sono pubbliche. La regola è NON_COMPLIANT se il campo è impostato su true. PubliclyAccessible

Identificatore: DMS_REPLICATION_NOT_PUBLIC

Tipi di risorse: AWS::DMS::ReplicationInstance

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dms-replication-task-sourcedb-logging

Verifica se la registrazione è abilitata con un livello di gravità valido per le attività di replica AWS DMS di un database di origine. La regola è NON_COMPLIANT se la registrazione di log non è abilitata o se i log per le attività di replica DMS di un database di origine hanno un livello di gravità non valido.

Identificatore: DMS_REPLICATION_TASK_SOURCEDB_LOGGING

Tipi di risorse: AWS::DMS::ReplicationTask

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dms-replication-task-targetdb-logging

Verifica se la registrazione è abilitata con un livello di gravità valido per gli eventi delle attività di replica AWS DMS di un database di destinazione. La regola è NON_COMPLIANT se la registrazione di log non è abilitata o se la registrazione di log delle attività di replica di un database di destinazione ha un livello di gravità non valido.

Identificatore: DMS_REPLICATION_TASK_TARGETDB_LOGGING

Tipi di risorse: AWS::DMS::ReplicationTask

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

docdb-cluster-audit-logging-enabled

Verifica se un cluster di istanze Amazon DocumentDB (con compatibilità MongoDB) ha l'esportazione dei log abilitata per i CloudWatch log di controllo. La regola è NON_COMPLIANT se un cluster di istanze Amazon DocumentDB non ha l'esportazione dei log abilitata per i CloudWatch log di controllo.

Identificatore: DOCDB_CLUSTER_AUDIT_LOGGING_ENABLED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile soltanto nelle regioni Asia Pacifico (Mumbai), Europa (Parigi), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Europa (Londra), Europa (Milano), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Centrale), Cina (Ningxia)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

docdb-cluster-backup-retention-check

Verifica se il periodo di conservazione del cluster di database Amazon Document è impostato su un numero di giorni specifico. La regola è NON_COMPLIANT se il periodo di conservazione è inferiore al valore specificato dal parametro.

Identificatore: DOCDB_CLUSTER_BACKUP_RETENTION_CHECK

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile soltanto nelle regioni Asia Pacifico (Mumbai), Europa (Parigi), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Europa (Londra), Europa (Milano), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Centrale), Cina (Ningxia)

Parametri:

minimo BackupRetentionPeriod (opzionale), Tipo: int

> Numero minimo di giorni in cui conservare i backup. I valori validi vanno da 1 a 35 e il valore predefinito è 7. Questa regola è NON_COMPLIANT se il valore è maggiore di 'backup'. RetentionPeriod

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

docdb-cluster-deletion-protection-enabled

Verifica se la protezione dall'eliminazione è abilitata per i cluster Amazon DocumentDB (compatibile con MongoDB). La regola è NON_COMPLIANT se il campo deletionProtection del cluster Amazon DocumentDB è impostato su false.

Identificatore: DOCDB_CLUSTER_DELETION_PROTECTION_ENABLED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile soltanto nelle regioni Asia Pacifico (Mumbai), Europa (Parigi), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Europa (Londra), Europa (Milano), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Centrale), Cina (Ningxia)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

docdb-cluster-encrypted

Verifica se la crittografia di archiviazione è abilitata per i cluster Amazon DocumentDB (compatibile con MongoDB). La regola è NON_COMPLIANT se la crittografia di archiviazione non è abilitata.

Identificatore: DOCDB_CLUSTER_ENCRYPTED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile soltanto nelle regioni Asia Pacifico (Mumbai), Europa (Parigi), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Europa (Londra), Europa (Milano), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Centrale), Cina (Ningxia)

Parametri:

kmsKeyArns (Opzionale), Tipo: CSV

> Un elenco separato da virgole di ARN di chiavi KMS da confrontare con l' KmsKeyID del cluster crittografato.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

docdb-cluster-snapshot-public-prohibited

Verifica se gli snapshot manuali dei cluster Amazon DocumentDB sono pubblici. La regola è NON_COMPLIANT se uno degli snapshot manuali dei cluster Amazon DocumentDB è pubblico.

Identificatore: DOCDB_CLUSTER_SNAPSHOT_PUBLIC_PROIBITED

Tipi di risorse: AWS: :RDS: :DB ClusterSnapshot

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile soltanto nelle regioni Asia Pacifico (Mumbai), Europa (Parigi), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Europa (Londra), Europa (Milano), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Centrale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dynamodb-autoscaling-enabled

Verifica se le tabelle o gli indici secondari globali Amazon DynamoDB possono elaborare la capacità di lettura/scrittura utilizzando la modalità on demand o la modalità con provisioning con il dimensionamento automatico abilitato. La regola è NON_COMPLIANT se una delle due modalità viene utilizzata senza il dimensionamento automatico abilitato

Identificatore: DYNAMODB_AUTOSCALING_ENABLED

Tipi di risorse: AWS::DynamoDB::Table

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

min ProvisionedReadCapacity (opzionale), Tipo: int

Il numero minimo di unità che devono essere sottoposte a provisioning con la capacità di lettura nel gruppo con dimensionamento automatico.

max ProvisionedReadCapacity (opzionale), Tipo: int

Il numero massimo di unità che devono essere sottoposte a provisioning con la capacità di lettura nel gruppo con dimensionamento automatico.

targetReadUtilization (Opzionale), Tipo: doppio

La percentuale di utilizzo di destinazione per la capacità di lettura. L'utilizzo di destinazione viene espresso come proporzione tra la capacità utilizzata e la capacità assegnata.

min ProvisionedWriteCapacity (opzionale), Tipo: int

Il numero minimo di unità che devono essere sottoposte a provisioning con la capacità di scrittura nel gruppo con dimensionamento automatico.

max ProvisionedWriteCapacity (opzionale), Tipo: int

Il numero massimo di unità che devono essere sottoposte a provisioning con la capacità di scrittura nel gruppo con dimensionamento automatico.

targetWriteUtilization (Opzionale), Tipo: doppio

La percentuale di utilizzo di destinazione per la capacità di scrittura. L'utilizzo di destinazione viene espresso come proporzione tra la capacità utilizzata e la capacità assegnata.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dynamodb-in-backup-plan

Verifica se la tabella Amazon DynamoDB è presente nei AWS piani di backup. La regola è NON_COMPLIANT se le tabelle Amazon DynamoDB non sono presenti in alcun piano di Backup. AWS

Identificatore: DYNAMODB_IN_BACKUP_PLAN

Tipi di risorse: AWS::DynamoDB::Table

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dynamodb-last-backup-recovery-point-created

Verifica se è stato creato un punto di ripristino per le tabelle Amazon DynamoDB entro il periodo specificato. La regola è NON_COMPLIANT se la tabella DynamoDB non dispone di un punto di ripristino corrispondente creato entro il periodo di tempo specificato.

Identificatore: DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipi di risorse: AWS::DynamoDB::Table

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▪Tipo: stringa

Tag delle tabelle DynamoDB che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▪Tipo: stringa

Nome della tabella DynamoDB che la regola deve verificare.

ripristino PointAgeValue (opzionale), Tipo: int, Impostazione predefinita: 1

Valore numerico per la durata massima consentita. Non superiore a 744 per le ore e 31 per i giorni.

ripristino PointAgeUnit (opzionale), ▪Tipo: stringa, Impostazione predefinita: giorni

Unità di tempo per la durata massima consentita. Valori accettati: "ore", "giorni".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

dynamodb-meets-restore-time-target

Verifica se il tempo di ripristino delle tabelle Amazon DynamoDB soddisfa la durata specificata. La regola è NON_COMPLIANT se LatestRestoreExecutionTimeMinutes una tabella DynamoDB supera i minuti. maxRestoreTime

Identificatore: DYNAMODB_MEETS_RESTORE_TIME_TARGET

Tipi di risorse: AWS::DynamoDB::Table

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

max RestoreTime, Tipo: int

Valore numerico per il runtime massimo di ripristino consentito.

resourceTags (opzionale), ▪Tipo: stringa

Tag delle tabelle DynamoDB che la regola deve verificare, in formato JSON.

resourceId (opzionale), ▪Tipo: stringa

Nome della tabella DynamoDB che la regola deve verificare.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dynamodb-pitr-enabled

Verifica se point-in-time il ripristino (PITR) è abilitato per le tabelle Amazon DynamoDB. La regola è NON_COMPLIANT se il PITR non è abilitato per le tabelle DynamoDB.

Identificatore: DYNAMODB_PITR_ENABLED

Tipi di risorse: AWS::DynamoDB::Table

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dynamodb-resources-protected-by-backup-plan

Verifica se le tabelle Amazon DynamoDB sono protette da un piano di backup. La regola è NON_COMPLIANT se le tabelle DynamoDB non sono coperte da un piano di backup.

Identificatore: DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipi di risorse: AWS::DynamoDB::Table

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▬Tipo: stringa

Tag per le tabelle DynamoDB che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▬Tipo: stringa

Nome della tabella DynamoDB che la regola deve verificare.

crossRegionList (Facoltativo), ▬Tipo: stringa

Elenco separato da virgole delle regioni di destinazione della copia di backup tra regioni da conservare

crossAccountList (Opzionale), ▬Tipo: stringa

Elenco separato da virgole degli account di destinazione della copia di backup tra account da conservare

maxRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione massimo in giorni per Vault Lock di Backup

minRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione minimo in giorni per Vault Lock di Backup

backup VaultLockCheck (opzionale), ▬Tipo: stringa

Valori accettati: "True" o "False". Immetti "True" per fare in modo che la regola verifichi se per la risorsa viene eseguito il backup in un vault bloccato

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dynamodb-table-deletion-protection-enabled

Verifica se la protezione dall'eliminazione è abilitata per le tabelle Amazon DynamoDB. La regola è NON_COMPLIANT se la protezione dall'eliminazione è disabilitata per le tabelle.

Identificatore: DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

Tipi di risorse: AWS::DynamoDB::Table

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dynamodb-table-encrypted-kms

Verifica se la tabella Amazon DynamoDB è crittografata AWS con Key Management Service (KMS). La regola è NON_COMPLIANT se la tabella Amazon DynamoDB non è crittografata con KMS. AWS La regola è anche NON_COMPLIANT se la chiave KMS crittografata non è presente nel parametro di input. AWS `kmsKeyArns`

Identificatore: DYNAMODB_TABLE_ENCRYPTED_KMS

Tipi di risorse: AWS::DynamoDB::Table

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsKeyArns (Facoltativo), Tipo: CSV

Elenco separato da virgole di ARN di chiavi AWS KMS consentite per crittografare le tabelle Amazon DynamoDB.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dynamodb-table-encryption-enabled

Verifica se le tabelle Amazon DynamoDB sono crittografate e ne controlla lo stato. La regola è COMPLIANT se lo stato è abilitato o in corso di abilitazione.

Identifier (Identificatore): DYNAMODB_TABLE_ENCRYPTION_ENABLED

Tipi di risorse: AWS::DynamoDB::Table

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

dynamodb-throughput-limit-check

Verifica se la velocità di trasmissione effettiva assegnata a DynamoDB si sta avvicinando al limite massimo per l'account. Per impostazione predefinita, la regola verifica se la velocità di trasmissione effettiva assegnata supera una soglia dell'80% dei limiti per l'account.

Identificatore: DYNAMODB_THROUGHPUT_LIMIT_CHECK

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

AccountRCU (opzionale) ThresholdPercentage , Tipo: int, Impostazione predefinita: 80

Percentuale di unità di capacità in lettura assegnate per l'account. Quando questo valore viene raggiunto, la regola viene contrassegnata come non conforme.

ThresholdPercentage AccountWCU (opzionale), Tipo: int, Impostazione predefinita: 80

Percentuale di unità di capacità in scrittura assegnate per l'account. Quando questo valore viene raggiunto, la regola viene contrassegnata come non conforme.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ebs-in-backup-plan

Verifica se i volumi Amazon Elastic Block Store (Amazon EBS) sono stati aggiunti nei piani di backup di Backup. AWS La regola è NON_COMPLIANT se i volumi Amazon EBS non sono inclusi nei piani di backup.

Identificatore: EBS_IN_BACKUP_PLAN

Tipi di risorse: AWS::EC2::Volume

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ebs-last-backup-recovery-point-created

Verifica se è stato creato un punto di ripristino per Amazon Elastic Block Store (Amazon EBS). La regola è NON_COMPLIANT se il volume Amazon EBS non dispone di un punto di ripristino corrispondente creato entro il periodo di tempo specificato.

Identificatore: EBS_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipi di risorse: AWS::EC2::Volume

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▪Tipo: stringa

Tag dei volumi Amazon EBS che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▪Tipo: stringa

ID del volume Amazon EBS che la regola deve verificare.

ripristino PointAgeValue (opzionale), Tipo: int, Impostazione predefinita: 1

Valore numerico per la durata massima consentita. Non superiore a 744 per le ore e 31 per i giorni.

ripristino PointAgeUnit (opzionale), ▪Tipo: stringa, Impostazione predefinita: giorni

Unità di tempo per la durata massima consentita. Valori accettati: "ore", "giorni".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation].

ebs-meets-restore-time-target

Controlla se il tempo di ripristino dei volumi Amazon Elastic Block Store (Amazon EBS) soddisfa la durata specificata. La regola è NON_COMPLIANT se LatestRestoreExecutionTimeMinutes un volume Amazon EBS supera i minuti. maxRestoreTime

Identificatore: EBS_MEETS_RESTORE_TIME_TARGET

Tipi di risorse: AWS::EC2::Volume

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

max RestoreTime, Tipo: int

Valore numerico per il runtime massimo di ripristino consentito.

resourceTags (opzionale), ▪Tipo: stringa

Tag per i volumi Amazon EBS che la regola deve verificare, in formato JSON.

resourceId (opzionale), ▪Tipo: stringa

ID del volume Amazon EBS che la regola deve verificare.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ebs-optimized-instance

Verifica se l'ottimizzazione Amazon EBS è abilitata per le istanze Amazon Elastic Compute Cloud (Amazon EC2) che possono essere ottimizzate per Amazon EBS. La regola è NON_COMPLIANT se l'ottimizzazione EBS non è abilitata per un'istanza Amazon EC2 che può essere ottimizzata per EBS.

> **Note**
>
> Le istanze EC2 ottimizzate per EBS per impostazione predefinita determinano sempre valutazioni delle regole che restituiscono `COMPLIANT`.

Identifier (Identificatore): EBS_OPTIMIZED_INSTANCE

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ebs-resources-protected-by-backup-plan

Verifica se i volumi Amazon Elastic Block Store (Amazon EBS) sono protetti da un piano di backup. La regola è NON_COMPLIANT se il volume Amazon EBS non è coperto da un piano di backup.

Identificatore: EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipi di risorse: AWS::EC2::Volume

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▬Tipo: stringa

Tag per i volumi Amazon EBS che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▬Tipo: stringa

ID del volume Amazon EBS che la regola deve verificare.

crossRegionList (Facoltativo), ▬Tipo: stringa

Elenco separato da virgole delle regioni di destinazione della copia di backup tra regioni da conservare

crossAccountList (Opzionale), ▬Tipo: stringa

Elenco separato da virgole degli account di destinazione della copia di backup tra account da conservare

maxRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione massimo in giorni per Vault Lock di Backup

minRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione minimo in giorni per Vault Lock di Backup

backup VaultLockCheck (opzionale), ➖Tipo: stringa

Valori accettati: "True" o "False". Immetti "True" per fare in modo che la regola verifichi se per la risorsa viene eseguito il backup in un vault bloccato

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ebs-snapshot-public-restorable-check

Verifica se gli snapshot Amazon Elastic Block Store (Amazon EBS) non sono ripristinabili pubblicamente. La regola è NON_COMPLIANT se uno o più snapshot con RestorableByUserIds campo sono impostati su tutti, ovvero gli snapshot di Amazon EBS sono pubblici.

Identificatore: EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

Tipo di trigger: Periodico

Regione AWS: tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-client-vpn-connection-log-enabled

Verifica se l'endpoint AWS Client VPN ha abilitato la registrazione della connessione client. La regola è NON_COMPLIANT se 'Configuration. ConnectionLogOptions.Enabled' è impostato su false.

Identificatore: EC2_CLIENT_VPN_CONNECTION_LOG_ENABLED

Tipi di risorse: Endpoint AWS::EC2::ClientVpn

Tipo di trigger: Modifiche alla configurazione

Regione AWS: tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-client-vpn-not-authorize-all

Verifica se le regole di autorizzazione AWS Client VPN autorizzano l'accesso alla connessione per tutti i client. La regola è NON_COMPLIANT se 'AccessAll' è presente e impostato su true.

Identificatore: EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL

Tipi di risorse: Endpoint AWS::EC2::ClientVpn

Tipo di trigger: Periodico

Regione AWS: tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-ebs-encryption-by-default

Verifica se la crittografia Amazon Elastic Block Store (EBS) è abilitata per impostazione predefinita. La regola è NON_COMPLIANT se la crittografia non è abilitata.

Identificatore: EC2_EBS_ENCRYPTION_BY_DEFAULT

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-imdsv2-check

Verifica se la versione dei metadati dell'istanza Amazon Elastic Compute Cloud (Amazon EC2) è configurata con il servizio di metadati di istanza versione 2 (IMDSv2). La regola è NON_COMPLIANT se è impostata su opzionale. HttpTokens

Identificatore: EC2_IMDSV2_CHECK

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-instance-detailed-monitoring-enabled

Verifica se il monitoraggio dettagliato è abilitato per le istanze EC2. La regola è NON_COMPLIANT se il monitoraggio dettagliato non è abilitato.

Identificatore: EC2_INSTANCE_DETAILED_MONITORING_ENABLED

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

ec2-instance-managed-by-systems-manager

> **Important**
>
> Per questa regola, l'identificatore (EC2_INSTANCE_MANAGED_BY_SSM) e il nome della regola (ec2-instance-managed-by-systems-manager) sono diversi.

Verifica se le tue istanze Amazon EC2 sono gestite da un AWS Systems Manager agente (agente SSM). La regola è NON_COMPLIANT se un'istanza EC2 è in esecuzione e l'agente SSM è arrestato, o se un'istanza EC2 è in esecuzione e l'agente SSM è terminato.

> **Note**
>
> La regola non restituirà NON_COMPLIANT se un'istanza EC2 viene arrestata e l'agente SSM è in esecuzione.

Identificatore: EC2_INSTANCE_MANAGED_BY_SSM

Tipi AWS::EC2::Instance, AWS::SSM::ManagedInstance di risorse: Inventario

Tipo di trigger: Modifiche alla configurazione

Regione AWS: tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-instance-multiple-eni-check

Verifica se Amazon Elastic Compute Cloud (Amazon EC2) utilizza più interfacce di rete elastiche (ENI) o Elastic Fabric Adapter (EFA). La regola è NON_COMPLIANT se un'istanza Amazon EC2 utilizza più interfacce di rete.

Identificatore: EC2_INSTANCE_MULTIPLE_ENI_CHECK

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

NetworkInterfaceIds (Facoltativo), Tipo: CSV

Elenco separato da virgole degli ID dell'istanza di rete

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
```

```
{
   "NetworkInterfaces": "[NetworkInterfaceId-1, NetworkInterfaceId-2,
 NetworkInterfaceId-3, ...]"
}
...
```

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-instance-no-public-ip

Verifica se per le istanze EC2 è presente un'associazione IP pubblica. La regola è NON_COMPLIANT se il campo publicIp è presente nell'elemento di configurazione dell'istanza EC2. Questa regola si applica solo a IPv4.

Contesto: gli indirizzi IP pubblici possono rendere le istanze EC2 direttamente accessibili da Internet, il che potrebbe non essere sempre auspicabile dal punto di vista della sicurezza o della conformità:

- Sicurezza: in molti casi, potrebbe non essere consigliabile che le istanze EC2 abbiano indirizzi IP pubblici, a meno che non sia necessario renderle accessibili pubblicamente. Avere un indirizzo IP pubblico può esporre l'istanza EC2 a potenziali rischi per la sicurezza, come attacchi o accessi non autorizzati.
- Conformità: diversi standard di conformità come PCI, DSS o HIPAA hanno requisiti specifici per quanto riguarda la segmentazione della rete e il controllo degli accessi. Garantire che le istanze EC2 non abbiano indirizzi IP pubblici non necessari può contribuire a garantire la conformità con questi requisiti.
- Gestione dei costi: gli indirizzi IP pubblici possono comportare costi aggiuntivi, soprattutto in presenza di istanze EC2 continuamente associate ad essi. Identificando le istanze EC2 con IP pubblici non necessari, puoi potenzialmente ridurre i costi.

Identificatore: EC2_INSTANCE_NO_PUBLIC_IP

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-instance-profile-attached

Verifica se a un'istanza EC2 è associato un profilo AWS Identity and Access Management (IAM). La regola è NON_COMPLIANT se all'istanza EC2 non è collegato alcun profilo IAM.

Identificatore: EC2_INSTANCE_PROFILE_ATTACHED

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

IamInstanceProfileArnList (Facoltativo), Tipo: CSV

> Elenco separato da virgole dei nomi della risorsa Amazon (ARN) del profilo IAM che possono essere collegati alle istanze Amazon EC2.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-last-backup-recovery-point-created

Verifica se è stato creato un punto di ripristino per le istanze Amazon Elastic Compute Cloud (Amazon EC2). La regola è NON_COMPLIANT se l'istanza Amazon EC2 non dispone di un punto di ripristino corrispondente creato entro il periodo di tempo specificato.

Identificatore: EC2_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▬Tipo: stringa

Tag delle istanze Amazon EC2 che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▬Tipo: stringa

ID dell'istanza Amazon EC2 che la regola deve verificare.

ripristino PointAgeValue (opzionale), Tipo: int, Impostazione predefinita: 1

Valore numerico per la durata massima consentita. Non superiore a 744 per le ore e 31 per i giorni.

ripristino PointAgeUnit (opzionale), ▬Tipo: stringa, Impostazione predefinita: giorni

Unità di tempo per la durata massima consentita. Valori accettati: "ore", "giorni".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

ec2-launch-template-public-ip-disabled

Verifica se i modelli di avvio di Amazon EC2 sono impostati sull'assegnazione di indirizzi IP pubblici alle interfacce di rete. La regola è NON_COMPLIANT se la versione predefinita di un EC2 Launch Template ha almeno un'interfaccia di rete con '' impostato su 'true'. AssociatePublic IpAddress

Identificatore: EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED

Tipi di risorse: AWS::EC2::LaunchTemplate

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

exemptedLaunchTemplates (Facoltativo), Tipo: CSV

Elenco separato da virgole di EC2 Launch Template ID esentati a cui è consentito avere interfacce di rete con il valore impostato su «true». AssociatePublicIpAddress

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-managedinstance-applications-blacklisted

Verifica se nessuna delle applicazioni specificate è installata nell'istanza. Facoltativamente, specifica la versione. Le versioni più recenti non verranno inserite nell'elenco negazione. Facoltativamente, specifica la piattaforma in modo da applicare la regola solo alle istanze in esecuzione in tale piattaforma.

Identificatore: EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

Tipi di risorse: AWS::SSM::ManagedInstance Inventario

Tipo di trigger: Modifiche alla configurazione

Regione AWS: tutte le AWS regioni supportate

Parametri:

applicationNames, Tipo: CSV

Elenco di nomi di applicazione separati da virgole. Facoltativamente, puoi specificare le versioni aggiunte con ":" (ad esempio "Chrome:0.5.3, FireFox").

> **Note**
>
> I nomi dell'applicazione devono corrispondere con esattezza. Ad esempio, puoi usare **`firefox`** in Linux o **`firefox-compat`** su Amazon Linux. Inoltre, attualmente non

AWS Config supporta i caratteri jolly per il parametro ApplicationNames (ad esempio,). **`firefox*`**

platformType (opzionale), ▬Tipo: stringa

Il tipo di piattaforma (ad esempio "Linux" o "Windows").

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-managedinstance-applications-required

Verifica se tutte le applicazioni specificate sono installate nell'istanza. Eventualmente, specifica la versione minima accettabile. Puoi anche specificare la piattaforma, in modo da applicare la regola solo alle istanze in esecuzione in tale piattaforma.

> **Note**
>
> Assicurati che l'agente SSM sia in esecuzione sull'istanza EC2 e che venga creata un'associazione per raccogliere l'inventario del software applicativo. La regola restituisce NOT_APPLICABLE se l'agente SSM non è installato o se un'associazione non è ancora stata creata o non è ancora in esecuzione.

Identificatore: EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED

Tipi di risorse: AWS::SSM::ManagedInstance Inventario

Tipo di trigger: Modifiche alla configurazione

Regione AWS: tutte le AWS regioni supportate

Parametri:

applicationNames, Tipo: CSV

Elenco di nomi di applicazione separati da virgole. Facoltativamente, puoi specificare le versioni aggiunte con ":" (ad esempio "Chrome:0.5.3, FireFox").

> **Note**
>
> I nomi dell'applicazione devono corrispondere con esattezza. Ad esempio, puoi usare **`firefox`** in Linux o **`firefox-compat`** su Amazon Linux. Inoltre, attualmente non AWS Config supporta i caratteri jolly per il parametro ApplicationNames (ad esempio,). **`firefox*`**

platformType (opzionale), ▬Tipo: stringa

Il tipo di piattaforma (ad esempio "Linux" o "Windows").

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-managedinstance-association-compliance-status-check

Verifica se lo stato di conformità dell'associazione AWS Systems Manager è CONFORME o NON_COMPLIANT dopo l'esecuzione dell'associazione sull'istanza. Se la regola è conforme, il campo mostra lo stato CONFORME. Per ulteriori informazioni sulle associazioni, consulta Che cos'è un'associazione?.

Identificatore: EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

Tipi di risorse: AWS::SSM::AssociationCompliance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-managedinstance-inventory-blacklisted

Verifica se le istanze gestite da Amazon EC2 Systems Manager sono configurate per raccogliere i tipi di inventario inseriti nelle blacklist.

Identificatore: EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED

Tipi di risorse: AWS::SSM::ManagedInstance Inventario

Tipo di trigger: Modifiche alla configurazione

Regione AWS: tutte le AWS regioni supportate

Parametri:

inventoryNames, Tipo: CSV

Elenco separato da virgole dei tipi di inventario di Systems Manager (ad esempio, ':Network AWS,: AWS'). WindowsUpdate

platformType (opzionale), ▬Tipo: stringa

Tipo di piattaforma (ad esempio "Linux").

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-managedinstance-patch-compliance-status-check

Verifica se lo stato di conformità della patch di AWS Systems Manager è CONFORME o NON_COMPLIANT dopo l'installazione della patch sull'istanza. Se la regola è conforme, il campo mostra lo stato CONFORME.

Identificatore: EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK

Tipi di risorse: AWS::SSM::PatchCompliance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-managedinstance-platform-check

Verifica se le istanze gestite di EC2 hanno le configurazioni desiderate.

Identificatore: EC2_MANAGEDINSTANCE_PLATFORM_CHECK

Tipi di risorse: AWS::SSM::ManagedInstance Inventario

Tipo di trigger: Modifiche alla configurazione

Regione AWS: tutte le AWS regioni supportate

Parametri:

platformType, ▪Tipo: stringa

Tipo di piattaforma (ad esempio "Linux").

platformVersion (opzionale), ▪Tipo: stringa

La versione della piattaforma (ad esempio "2016.09").

agentVersion (opzionale), ▪Tipo: stringa

La versione dell'agente (ad esempio "2.0.433.0").

platformName (opzionale), ▪Tipo: stringa

La versione della piattaforma (ad esempio "2016.09")

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-meets-restore-time-target

Controlla se il tempo di ripristino delle istanze Amazon Elastic Compute Cloud (Amazon EC2) soddisfa la durata specificata. La regola è NON_COMPLIANT se un'istanza LatestRestoreExecutionTimeMinutes Amazon EC2 dura più di minuti. maxRestoreTime

Identificatore: EC2_MEETS_RESTORE_TIME_TARGET

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

max RestoreTime, Tipo: int

Valore numerico per il runtime massimo di ripristino consentito.

resourceTags (opzionale), ▪Tipo: stringa

Tag delle istanze Amazon EC2 che la regola deve verificare, in formato JSON.

resourceId (opzionale), ▪Tipo: stringa

ID dell'istanza Amazon EC2 che la regola deve verificare.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

ec2-no-amazon-key-pair

Verifica se le istanze Amazon Elastic Compute Cloud (EC2) in esecuzione vengono avviate tramite le coppie di chiavi Amazon. La regola è NON_COMPLIANT se un'istanza EC2 in esecuzione viene avviata con una coppia di chiavi.

Identificatore: EC2_NO_AMAZON_KEY_PAIR

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-paravirtual-instance-check

Verifica se il tipo di virtualizzazione di un'istanza EC2 è paravirtuale. Questa regola è NON_COMPLIANT per un'istanza EC2 se "virtualizationType" è impostato su "paravirtual".

Identificatore: EC2_PARAVIRTUAL_INSTANCE_CHECK

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile soltanto nelle regioni Cina (Pechino), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), Asia Pacifico (Singapore), Asia Pacifico (Sydney)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-resources-protected-by-backup-plan

Verifica se le istanze Amazon Elastic Compute Cloud (Amazon EC2) sono protette da un piano di backup. La regola è NON_COMPLIANT se l'istanza Amazon EC2 non è coperta da un piano di backup.

> **Note**
>
> Questa regola è applicabile solo alle istanze Amazon EC2 in esecuzione e non a quelle disattivate.

Identificatore: EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▬Tipo: stringa

Tag per le istanze Amazon EC2 che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▬Tipo: stringa

ID dell'istanza Amazon EC2 che la regola deve verificare.

crossRegionList (Facoltativo), ▬Tipo: stringa

Elenco separato da virgole delle regioni di destinazione della copia di backup tra regioni da conservare

crossAccountList (Opzionale), ▬Tipo: stringa

Elenco separato da virgole degli account di destinazione della copia di backup tra account da conservare

maxRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione massimo in giorni per Vault Lock di Backup

minRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione minimo in giorni per Vault Lock di Backup

backup VaultLockCheck (opzionale), ▬Tipo: stringa

Valori accettati: "True" o "False". Immetti "True" per fare in modo che la regola verifichi se per la risorsa viene eseguito il backup in un vault bloccato

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-security-group-attached-to-eni

Verifica se i gruppi di sicurezza non predefiniti sono collegati alle interfacce di rete elastiche. La regola è NON_COMPLIANT se il gruppo di sicurezza non è associato a un'interfaccia di rete.

Identificatore: EC2_SECURITY_GROUP_ATTACHED_TO_ENI

Tipi di risorse: AWS::EC2::SecurityGroup

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-security-group-attached-to-eni-periodic

Verifica se i gruppi di sicurezza non predefiniti sono collegati alle interfacce di rete elastiche (ENI). La regola è NON_COMPLIANT se il gruppo di sicurezza non è associato a un'ENI. I gruppi di sicurezza non di proprietà dell'account che ha effettuato la chiamata vengono valutati come NOT_APPLICABLE.

> **Note**
>
> Questa regola riporta il tipo di risorsa `AWS::EC2::SecurityGroup`. Tuttavia, affinché la regola funzioni in modo efficace, è necessario abilitare la registrazione del tipo di risorsa `AWS::EC2::NetworkInterface`.

Identificatore: EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC

Tipi di risorse: AWS::EC2::SecurityGroup

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-stopped-instance

Verifica se sono presenti istanze Amazon Elastic Compute Cloud (Amazon EC2) interrotte per un numero di giorni maggiore rispetto al numero consentito. La regola è NON_COMPLIANT se lo stato di un'istanza Amazon EC2 è stato interrotto più a lungo del numero consentito di giorni o per un intervallo di tempo impossibile da determinare.

Identificatore: EC2_STOPPED_INSTANCE

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

AllowedDays (Facoltativo), Tipo: int, Impostazione predefinita: 30

Il numero di giorni in cui un'istanza Amazon EC2 può essere interrotta prima che la regola diventi NON_COMPLIANT. Il numero predefinito di giorni è 30.

> **Note**
>
> Il numero di giorni selezionato deve essere inferiore al periodo di conservazione configurato, poiché questa regola si basa sui dati storici raccolti. Per ulteriori informazioni sulla conservazione dei dati storici, vedere Eliminazione AWS Config dei dati.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-token-hop-limit-check

Verifica se il limite di hop del token specificato per i metadati di un'istanza Amazon Elastic Compute Cloud (EC2) è inferiore al limite desiderato. La regola è NON_COMPLIANT per un'istanza se il relativo limite di hop è superiore al limite previsto.

Identificatore: EC2_TOKEN_HOP_LIMIT_CHECK

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

tokenHopLimit (Facoltativo), Tipo: int

> Il limite di hop del token desiderato. I valori validi sono compresi tra 1 e 64 (inclusi). Se non viene specificato alcun valore per il parametro, il valore predefinito è 1.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-transit-gateway-auto-vpc-attach-disabled

Verifica se i gateway di transito Amazon Elastic Compute Cloud (Amazon EC2) hanno 'abilitato. AutoAccept SharedAttachments La regola è NON_COMPLIANT per un Transit Gateway se '' è impostato su AutoAccept SharedAttachments 'abilita'.

Identificatore: EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED

Tipi di risorse: AWS::EC2::TransitGateway

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Disponibile solo in Europa (Stoccolma), Europa (Parigi), Stati Uniti orientali (Ohio), Africa (Città del Capo), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Europa (Londra), Europa (Milano), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), Asia Pacifico Singapore (), Regione Asia Pacifico (Sydney), Canada (Centrale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-volume-inuse-check

Verifica se i volumi EBS sono collegati alle istanze EC2. Facoltativamente, verifica se i volumi EBS sono contrassegnati per l'eliminazione quando un'istanza viene terminata.

La regola è COMPLIANT se un volume EBS è collegato a un'istanza EC2 in esecuzione. In questo caso, è COMPLIANT quando il volume EBS viene utilizzato attivamente da un'istanza EC2.

La regola è NON_COMPLIANT se un volume EBS non è collegato a nessuna istanza EC2 o se è collegato a un'istanza EC2 interrotta o terminata. In questo caso, è NON_COMPLIANT quando il volume EBS non è utilizzato attivamente da un'istanza EC2.

Identificatore: EC2_VOLUME_INUSE_CHECK

Tipi di risorse: AWS::EC2::Volume

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

deleteOnTermination (Facoltativo), Tipo: booleano

> I volumi EBS sono contrassegnati per l'eliminazione quando un'istanza viene terminata. Valori possibili: True o False (gli altri valori di input sono contrassegnati come NON_COMPLIANT).

Se impostata su `True`, la regola è NON_COMPLIANT se un volume EBS terminato non è contrassegnato per l'eliminazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ecr-private-image-scanning-enabled

Verifica se la scansione delle immagini è abilitata per un repository Amazon Elastic Container Registry (Amazon ECR) privato. La regola è NON_COMPLIANT se la frequenza di scansione del repository Amazon ECR privato non è impostata sulla scansione su invio o sulla scansione continua. Per ulteriori informazioni sulla scansione delle immagini, consulta Scansione delle immagini nella Guida per l'utente di Amazon ECR.

Identificatore: ECR_PRIVATE_IMAGE_SCANNING_ENABLED

Tipi di risorse: AWS::ECR::Repository

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ecr-private-lifecycle-policy-configured

Verifica se per un repository Amazon Elastic Container Registry (ECR) privato è configurata almeno una policy del ciclo di vita. La regola è NON_COMPLIANT se non è configurata alcuna policy del ciclo di vita per il repository ECR privato.

Identificatore: ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED

Tipi di risorse: AWS::ECR::Repository

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ecr-private-tag-immutability-enabled

Verifica se per un repository Amazon Elastic Container Registry (ECR) privato è abilitata l'immutabilità dei tag. Questa regola è NON_COMPLIANT se l'immutabilità dei tag non è abilitata per il repository ECR privato.

Identificatore: ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

Tipi di risorse: AWS::ECR::Repository

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ecs-awsvpc-networking-enabled

Verifica se la modalità di rete per ECS attivo è impostata su 'awsvpc'. TaskDefinitions Questa regola è NON_COMPLIANT se ECS attivo non è impostato su 'awsvpc'. TaskDefinitions

> **Note**
> Questa regola valuta solo l'ultima revisione attiva di una definizione dell'attività Amazon ECS.

AWSVPC_NETWORKINGIdentificatore: ECS_ _ENABLED

Tipi di risorse: AWS::ECS::TaskDefinition

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ecs-containers-nonprivileged

Verifica se il parametro privilegiato nella definizione del contenitore di TaskDefinitions ECS è impostato su «true». La regola è NON_COMPLIANT se il parametro con privilegi è "true".

> **Note**
> Questa regola valuta solo l'ultima revisione attiva di una definizione dell'attività Amazon ECS.

Identificatore: ECS_CONTAINERS_NONPRIVILEGED

Tipi di risorse: AWS::ECS::TaskDefinition

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ecs-containers-readonly-access

Verifica se i container Amazon Elastic Container Service (Amazon ECS) hanno accesso in sola lettura ai relativi file system root. La regola è NON_COMPLIANT se il parametro nella definizione del contenitore di ECS è impostato su 'false'. readonlyRootFilesystem TaskDefinitions

> **Note**
>
> Questa regola valuta solo l'ultima revisione attiva di una definizione dell'attività Amazon ECS.

Identificatore: ECS_CONTAINERS_READONLY_ACCESS

Tipi di risorse: AWS::ECS::TaskDefinition

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ecs-container-insights-enabled

Verifica se le informazioni sui container sono abilitate per i cluster Amazon Elastic Container Service. La regola è NON_COMPLIANT se le informazioni sui container non sono abilitate.

Identificatore: ECS_CONTAINER_INSIGHTS_ENABLED

Tipi di risorse: AWS::ECS::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ecs-fargate-latest-platform-version

Verifica se i servizi Fargate ECS sono impostati sulla versione della piattaforma più recente. La regola è NON_COMPLIANT se per PlatformVersion il tipo di avvio Fargate non è impostato su LATEST o se nessuno dei due latestLinuxVersion viene fornito come parametro. `latestWindowsVersion`

Identificatore: ECS_FARGATE_LATEST_PLATFORM_VERSION

Tipi di risorse: AWS::ECS::Service

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

latestLinuxVersion (Facoltativo), ▪Tipo: stringa

> L'ultima versione di Linux supportata da PlatformVersion '' nel formato semantic versioning (SemVer). Il parametro può essere necessario se Fargate è stato distribuito e il parametro 'PlatformVersion' è stato specificato esplicitamente o CodeDeploy viene utilizzato come '' DeploymentController

latestWindowsVersion (Facoltativo), ▪Tipo: stringa

> L'ultima versione di Windows PlatformVersion supportava '' nel formato semantic versioning (SemVer). Il parametro può essere necessario se Fargate è stato distribuito e il parametro

'PlatformVersion' è stato specificato esplicitamente o CodeDeploy viene utilizzato come '' DeploymentController

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ecs-no-environment-secrets

Verifica se i segreti vengono trasmessi come variabili di ambiente del container. La regola è NON_COMPLIANT se 1 o più chiavi di variabile dell'ambiente corrispondono a una chiave elencata nel parametro "`secretKeys`" (escluse le variabili ambientali di altre posizioni come Amazon S3).

> **Note**
>
> Questa regola valuta solo l'ultima revisione attiva di una definizione dell'attività Amazon ECS.

Identificatore: ECS_NO_ENVIRONMENT_SECRETS

Tipi di risorse: AWS::ECS::TaskDefinition

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

secretKeys, Tipo: CSV

Elenco separato da virgole dei nomi delle chiavi da cercare nelle variabili di ambiente delle definizioni dei container all'interno delle definizioni delle attività. Gli spazi aggiuntivi verranno rimossi.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ecs-task-definition-log-configuration

Verifica se logConfiguration è impostato sulle definizioni delle attività ECS attive. Questa regola è NON_COMPLIANT se un ECS attivo non TaskDefinition ha la risorsa LogConfiguration definita o il valore per LogConfiguration è nullo in almeno una definizione di contenitore.

> **Note**
>
> Questa regola valuta solo l'ultima revisione attiva di una definizione dell'attività Amazon ECS.

Identificatore: ECS_TASK_DEFINITION_LOG_CONFIGURATION

Tipi di risorse: AWS::ECS::TaskDefinition

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

ecs-task-definition-memory-hard-limit

Verifica se per le definizioni delle attività Amazon Elastic Container Service (ECS) è impostato un limite di memoria per le relative definizioni dei container. La regola è NON_COMPLIANT per una definizione delle attività se il parametro "memory" è assente per una definizione del container.

> **Note**
>
> Questa regola valuta solo l'ultima revisione attiva di una definizione dell'attività Amazon ECS.

Identificatore: ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT

Tipi di risorse: AWS::ECS::TaskDefinition

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ecs-task-definition-nonroot-user

Verifica se ECS TaskDefinitions specifica un utente per i contenitori di tipo di avvio Amazon Elastic Container Service (Amazon ECS) EC2 su cui eseguire. La regola è NON_COMPLIANT se il parametro "user" non è presente o se è impostato su "root".

> **Note**
>
> Questa regola valuta solo l'ultima revisione attiva di una definizione dell'attività Amazon ECS.

Identificatore: ECS_TASK_DEFINITION_NONROOT_USER

Tipi di risorse: AWS::ECS::TaskDefinition

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ecs-task-definition-pid-mode-check

Verifica se ECS è TaskDefinitions configurato per condividere lo spazio dei nomi dei processi di un host con i relativi contenitori Amazon Elastic Container Service (Amazon ECS). La regola è NON_COMPLIANT se il parametro pidMode è impostato su "host".

> **Note**
>
> Questa regola valuta solo l'ultima revisione attiva di una definizione dell'attività Amazon ECS.

Identificatore: ECS_TASK_DEFINITION_PID_MODE_CHECK

Tipi di risorse: AWS::ECS::TaskDefinition

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

ecs-task-definition-user-for-host-mode-check

Verifica se sono presenti autorizzazioni non autorizzate nelle definizioni dell'attività Amazon Elastic Container Service (Amazon ECS) più recenti attive con il parametro `NetworkMode` impostato su "host". La regola è NON_COMPLIANT per le definizioni delle attività con il parametro `NetworkMode` impostato su host e per le definizioni dei container di `privileged` impostate su false o su empty e di `user` impostate su root o su empty.

> **Important**
>
> È consigliato rimuovere i privilegi elevati dalle definizioni delle attività di Amazon ECS. Quando `privileged` è vero, al contenitore vengono concesse autorizzazioni elevate

sull'istanza del contenitore host (simili all'`root`utente). Quando si eseguono attività che utilizzano la modalità di rete `host`, per una maggiore sicurezza, non eseguire container utilizzando l'utente root (UID 0). Come best practice per la sicurezza, utilizza sempre un utente non root.

Identificatore: ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

Tipi di risorse: AWS::ECS::TaskDefinition

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

SkipInactiveTaskDefinitions (Facoltativo), Tipo: booleano

Flag booleano per escludere dalla verifica le definizioni delle attività Amazon EC2 nello stato INACTIVE. Se impostata su "true", la regola non valuta le definizioni delle attività di Amazon EC2 nello stato INACTIVE. Se impostata su "false", la regola valuta la revisione più recente delle definizioni delle attività di Amazon EC2 nello stato INACTIVE.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

efs-access-point-enforce-root-directory

Verifica se i punti di accesso Amazon Elastic File System (Amazon EFS) sono configurati sull'imposizione di una directory root. La regola è NON_COMPLIANT se il valore di "Path" è impostato su "/" (directory root predefinita del file system).

Identificatore: EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

Tipi di risorse: AWS::EFS::AccessPoint

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

approvedDirectories (opzionale), Tipo: CSV

Elenco separato da virgole dei percorsi delle sottodirectory approvati per l'imposizione della directory root del punto di accesso Amazon EFS.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

efs-access-point-enforce-user-identity

Verifica se i punti di accesso Amazon Elastic File System (Amazon EFS) sono configurati sull'imposizione di un'identità utente. La regola è NON_COMPLIANT se 'PosixUser' non è definito o se vengono forniti parametri e non c'è corrispondenza nel parametro corrispondente.

Identificatore: EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY

Tipi di risorse: AWS::EFS::AccessPoint

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

approvedUids (opzionale), Tipo: CSV

Elenco separato da virgole degli ID utente POSIX approvati per l'imposizione utente del punto di accesso EFS.

approvedGids (opzionale), Tipo: CSV

Elenco separato da virgole degli ID del gruppo POSIX approvati per l'imposizione utente del punto di accesso EFS.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

efs-encrypted-check

Verifica se Amazon Elastic File System (Amazon EFS) è configurato per crittografare i dati dei file utilizzando AWS Key Management Service (AWS KMS). La regola è NON_COMPLIANT se la chiave crittografata è impostata su false in `DescribeFileSystems` o se la chiave `KmsKeyId` in `DescribeFileSystems` non corrisponde al parametro `KmsKeyId`.

Identificatore: EFS_ENCRYPTED_CHECK

Tipi di risorse: AWS::EFS::FileSystem

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

KmsKeyId (Facoltativo), ▪Tipo: stringa

Nome della risorsa Amazon (ARN) della chiave KMS utilizzata per crittografare il file system EFS.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

efs-in-backup-plan

Verifica se i file system Amazon Elastic File System (Amazon EFS) sono stati aggiunti nei piani di backup di AWS Backup. La regola è NON_COMPLIANT se i file system EFS non sono inclusi nei piani di backup.

Identificatore: EFS_IN_BACKUP_PLAN

Tipi di risorse: AWS::EFS::FileSystem

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

efs-last-backup-recovery-point-created

Verifica se è stato creato un punto di ripristino per i file system Amazon Elastic File System (Amazon EFS). La regola è NON_COMPLIANT se il file system Amazon EFS non dispone di un punto di ripristino corrispondente creato entro il periodo di tempo specificato.

Identificatore: EFS_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipi di risorse: AWS::EFS::FileSystem

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▬Tipo: stringa

Tag dei file system Amazon EFS che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▬Tipo: stringa

ID del file system EFS che la regola deve verificare.

ripristino PointAgeValue (opzionale), Tipo: int, Impostazione predefinita: 1

Valore numerico per la durata massima consentita. Non superiore a 744 per le ore e 31 per i giorni.

ripristino PointAgeUnit (opzionale), ▬Tipo: stringa, Impostazione predefinita: giorni

Unità di tempo per la durata massima consentita. Valori accettati: "ore", "giorni".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

efs-meets-restore-time-target

Controlla se il tempo di ripristino dei volumi Amazon Elastic File System (Amazon EFS) soddisfa la durata specificata. La regola è NON_COMPLIANT se un file system LatestRestoreExecutionTimeMinutes Amazon EFS dura più di minuti. maxRestoreTime

Identificatore: EFS_MEETS_RESTORE_TIME_TARGET

Tipi di risorse: AWS::EFS::FileSystem

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

max RestoreTime, Tipo: int

Valore numerico per il runtime massimo di ripristino consentito.

resourceTags (opzionale), ▪Tipo: stringa

Tag dei file system Amazon EFS che la regola deve verificare, in formato JSON.

resourceId (opzionale), ▪Tipo: stringa

ID del file system EFS che la regola deve verificare.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

efs-mount-target-accessibile-pubblico

Verifica se un target di montaggio Amazon Elastic File System (Amazon EFS) non è associato a una sottorete pubblica. La regola non è conforme se la destinazione di montaggio di Amazon EFS è associata a una sottorete pubblica.

Identificatore: EFS_MOUNT_TARGET_PUBLIC_ACCESSIBLE

Tipi di risorse: AWS::EFS::FileSystem

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

efs-resources-protected-by-backup-plan

Verifica se i file system Amazon Elastic File System (Amazon EFS) sono protetti da un piano di backup. La regola è NON_COMPLIANT se il file system EFS non è coperto da un piano di backup.

Identificatore: EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipi di risorse: AWS::EFS::FileSystem

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▬Tipo: stringa

Tag dei file system EFS che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▬Tipo: stringa

ID del file system EFS che la regola deve verificare.

crossRegionList (Facoltativo), ▬Tipo: stringa

Elenco separato da virgole delle regioni di destinazione della copia di backup tra regioni da conservare

crossAccountList (Opzionale), ▬Tipo: stringa

Elenco separato da virgole degli account di destinazione della copia di backup tra account da conservare

maxRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione massimo in giorni per Vault Lock di Backup

minRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione minimo in giorni per Vault Lock di Backup

backup VaultLockCheck (opzionale), ➖Tipo: stringa

Valori accettati: "True" o "False". Immetti "True" per fare in modo che la regola verifichi se per la risorsa viene eseguito il backup in un vault bloccato

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

eip-attached

Verifica se tutti gli indirizzi IP elastici assegnati a un AWS account sono collegati a istanze EC2 o interfacce di rete elastiche in uso. La regola è NON_COMPLIANT se " AssociationId è nullo per l'indirizzo IP elastico.

> **Note**
>
> Dopo una valutazione, potrebbe essere necessario attendere anche 6 ore prima che i risultati siano resi disponibili.

Identificatore: EIP_ATTACHED

Tipi di risorse: AWS::EC2::EIP

Tipo di trigger: Modifiche alla configurazione

Regione AWS: AWS Tutte le regioni supportate

Parametri:

Nessuno

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
   "InstanceId": "my-instance-Id"
}
...
```

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

eks-cluster-logging-enabled

Verifica se un cluster Amazon Elastic Kubernetes Service (Amazon EKS) è configurato con la registrazione di log abilitata. La regola è NON_COMPLIANT se la registrazione di log per i cluster Amazon EKS non è abilitata per tutti i tipi di log.

Identificatore: EKS_CLUSTER_LOGGING_ENABLED

Tipi di risorse: AWS::EKS::Cluster

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

eks-cluster-log-enabled

Verifica se un cluster Amazon Elastic Kubernetes Service (Amazon EKS) è configurato con la registrazione di log abilitata. La regola è NON_COMPLIANT se la registrazione di log non è abilitata per i cluster Amazon EKS o se la registrazione di log non è abilitata con il tipo di log indicato.

Identificatore: EKS_CLUSTER_LOG_ENABLED

Tipi di risorse: AWS::EKS::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

logTypes (opzionale), Tipo: CSV

> Elenco separato da virgole dei tipi di log del piano di controllo del cluster EKS che devono essere abilitati.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

eks-cluster-oldest-supported-version

Verifica se un cluster Amazon Elastic Kubernetes Service (EKS) esegue la versione meno recente supportata. La regola è NON_COMPLIANT se un cluster EKS esegue la versione meno recente supportata (uguale al parametro "`oldestVersionSupported`").

Identificatore: EKS_CLUSTER_OLDEST_SUPPORTED_VERSION

Tipi di risorse: AWS::EKS::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

più vecchia VersionSupported, ➖Tipo: stringa

Valore della versione meno recente di Kubernetes supportata su AWS.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

eks-cluster-secrets-crittografato

Verifica se i cluster Amazon EKS sono configurati per avere segreti Kubernetes crittografati tramite KMS. AWS La regola è NON_COMPLIANT se un cluster EKS non dispone di una risorsa EncryptionConfig o se EncryptionConfig non nomina i segreti come risorsa.

Identificatore: EKS_CLUSTER_SECRETS_ENCRYPTED

Tipi di risorse: AWS::EKS::Cluster

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsKeyArns (Facoltativo), Tipo: CSV

Elenco separato da virgole di Amazon Resource Names (ARN) delle chiavi KMS approvate per l'utilizzo di EKS.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

eks-cluster-supported-version

Verifica se un cluster Amazon Elastic Kubernetes Service (EKS) esegue una versione di Kubernetes supportata. Questa regola è NON_COMPLIANT se un cluster EKS esegue una versione non supportata (inferiore al parametro "`oldestVersionSupported`").

Identificatore: EKS_CLUSTER_SUPPORTED_VERSION

Tipi di risorse: AWS::EKS::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

più vecchia VersionSupported, ➖Tipo: stringa

Valore della versione meno recente di Kubernetes supportata su AWS.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

eks-endpoint-no-public-access

Verifica se l'endpoint Amazon Elastic Kubernetes Service (Amazon EKS) non è accessibile pubblicamente. La regola è NON_COMPLIANT se l'endpoint è pubblicamente accessibile.

Identificatore: EKS_ENDPOINT_NO_PUBLIC_ACCESS

Tipi di risorse: AWS::EKS::Cluster

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

eks-secrets-encrypted

Verifica se i cluster Amazon Elastic Kubernetes Service sono configurati per avere segreti Kubernetes crittografati utilizzando chiavi (KMS). AWS Key Management Service

- Questa regola è COMPLIANT se un cluster EKS ha un parametro encryptionConfig con segreti uguali a una delle risorse.
- Questa regola è COMPLIANT anche se la chiave utilizzata per crittografare i segreti EKS corrisponde al parametro.
- Questa regola è NON_COMPLIANT se un cluster EKS non ha un parametro encryptionConfig o se le risorse encryptionConfig non includono segreti.
- Questa regola è NON_COMPLIANT anche se la chiave utilizzata per crittografare i segreti EKS non corrisponde al parametro.

Identificatore: EKS_SECRETS_ENCRYPTED

Tipi di risorse: AWS::EKS::Cluster

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsKeyArns (Facoltativo), Tipo: CSV

> Elenco separato da virgole dei nomi della risorsa Amazon (ARN) della chiave KMS che devono essere usati per i segreti crittografati in un cluster EKS.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

elasticache-auto-minor-version-upgrade-check

Verifica se i cluster Amazon ElastiCache for Redis hanno abilitato gli aggiornamenti automatici delle versioni secondarie. La regola è NON_COMPLIANT per un ElastiCache cluster se utilizza il motore Redis e '' non è impostato su 'true'. AutoMinor VersionUpgrade

Identificatore: ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

Tipi di risorse: AWS::ElastiCache::CacheCluster

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elasticache-rbac-auth-enabled

Verifica se i gruppi di ElastiCache replica Amazon hanno l'autenticazione RBAC abilitata. La regola è NON_COMPLIANT se la versione Redis è 6 o successiva e «UserGroupIds» è mancante, vuoto o non corrisponde a una voce fornita dal parametro ". `allowedUserGroupIDs`

Identificatore: ELASTICACHE_RBAC_AUTH_ENABLED

Tipi di risorse: AWS::ElastiCache::ReplicationGroup

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

UserGroupID consentiti (facoltativo), Tipo: CSV

> Un elenco separato da virgole di ID di gruppi di utenti approvati per l'accesso ai gruppi di ElastiCache replica.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elasticache-redis-cluster-automatic-backup-check

Verifica se i cluster Amazon ElastiCache Redis hanno attivato il backup automatico. La regola è NON_COMPLIANT se il cluster SnapshotRetentionLimit for Redis è inferiore al parametro. SnapshotRetentionPeriod Ad esempio: se il parametro è 15, la regola non è conforme se è compresa tra 0 e 15. snapshotRetentionPeriod

Identificatore: ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

Tipi di risorse:, AWS::ElastiCache::CacheCluster AWS::ElastiCache::ReplicationGroup

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

snapshotRetentionPeriod (Facoltativo), Tipo: int, Impostazione predefinita: 15

> Periodo di conservazione dello snapshot minimo in giorni per il cluster Redis. L'impostazione predefinita è 15 giorni.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

elasticache-repl-grp-auto-failover-enabled

Verifica se i gruppi di replica Amazon ElastiCache Redis hanno il failover automatico abilitato. La regola è NON_COMPLIANT per un gruppo di ElastiCache replica se '' non è impostato su 'abilitato'. AutomaticFailover

Identificatore: ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

Tipi di risorse: AWS::ElastiCache::ReplicationGroup

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elasticache-repl-grp-encrypted-at-rest

Verifica se i gruppi di ElastiCache replica Amazon sono encryption-at-rest abilitati. La regola è NON_COMPLIANT per un gruppo di ElastiCache replica se 'AtRestEncryptionEnabled' è disabilitato o se l'ARN della chiave KMS non corrisponde al parametro ApprovedKMS. KeyArns

Identificatore: ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

Tipi di risorse: AWS::ElastiCache::ReplicationGroup

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

KMS approvati (opzionale) KeyIds , Tipo: CSV

Elenco separato da virgole di ID chiave KMS approvati per l'uso. ElastiCache

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elasticache-repl-grp-encrypted-in-transit

Verifica se i gruppi di ElastiCache replica Amazon sono encryption-in-transit abilitati. La regola è NON_COMPLIANT per un gruppo di ElastiCache replica se 'Enabled' è impostato su 'false'. TransitEncryption

Identificatore: ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

Tipi di risorse: AWS::ElastiCache::ReplicationGroup

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elasticache-repl-grp-redis-auth-enabled

Verifica se i gruppi di ElastiCache replica Amazon hanno Redis AUTH abilitato. La regola è NON_COMPLIANT per un gruppo di ElastiCache replica se la versione Redis dei relativi nodi è inferiore a 6 (la versione 6+ utilizza gli ACL Redis) e '' è mancante o è vuoto/nullo. AuthToken

Identificatore: ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

Tipi di risorse: AWS::ElastiCache::ReplicationGroup

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elasticache-subnet-group-check

Verifica se ElastiCache i cluster Amazon sono configurati con un gruppo di sottoreti personalizzato. La regola è NON_COMPLIANT per un ElastiCache cluster se utilizza un gruppo di sottoreti predefinito.

Identificatore: ELASTICACHE_SUBNET_GROUP_CHECK

Tipi di risorse: AWS::ElastiCache::CacheCluster

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elasticache-supported-engine-version

Verifica se ElastiCache i cluster eseguono una versione superiore o uguale alla versione del motore consigliata. La regola è NON_COMPLIANT se il 'EngineVersion' di un ElastiCache cluster è inferiore alla versione consigliata specificata per il relativo motore.

Identificatore: ELASTICACHE_SUPPORTED_ENGINE_VERSION

Tipi di risorse: AWS::ElastiCache::CacheCluster

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

più recente MemcachedVersion, ▪Tipo: stringa

La versione più recente del motore consigliata per Memcached. I valori validi sono in formato semantic versioning (SemVer) con numero a 3 componenti per le versioni principali, secondarie e patch (ad esempio, 1.6.6, non 1.6).

più recente RedisVersion, ▪Tipo: stringa

La versione più recente del motore consigliata per Redis. I valori validi sono in formato semantic versioning (SemVer) con numero a 3 componenti per le versioni principali, secondarie e patch (ad esempio, 7.0.5, non 7.0).

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elasticsearch-encrypted-at-rest

Verifica se i domini Amazon OpenSearch Service (precedentemente chiamati Elasticsearch) hanno la configurazione Encryption at Rest abilitata. La regola è NON_COMPLIANT se il campo non è abilitato. EncryptionAtRestOptions

Identificatore: ELASTICSEARCH_ENCRYPTED_AT_REST

Tipi di risorse: AWS::Elasticsearch::Domain

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elasticsearch-in-vpc-only

Verifica se i domini Amazon OpenSearch Service (precedentemente chiamati Elasticsearch) si trovano in Amazon Virtual Private Cloud (Amazon VPC). La regola è NON_COMPLIANT se un endpoint del dominio Service è pubblico. OpenSearch

Identificatore: ELASTICSEARCH_IN_VPC_ONLY

Tipi di risorse: AWS::Elasticsearch::Domain

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elasticsearch-logs-to-cloudwatch

Verifica se i domini Amazon OpenSearch Service sono configurati per inviare log ad Amazon CloudWatch Logs. La regola è COMPLIANT se un log è abilitato per un dominio Amazon ES. Questa regola è NON_COMPLIANT se la registrazione di log non è configurata.

Identificatore: ELASTICSEARCH_LOGS_TO_CLOUDWATCH

Tipi di risorse: AWS::Elasticsearch::Domain

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

logTypes (opzionale), Tipo: CSV

Elenco separato da virgole dei log abilitati. I valori validi sono "search", "index", "error".

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
   "LogPublishingOptions": "{Key : Value, ...}"*
}
```

```
...
```

*Un oggetto con una o più delle seguenti chiavi: `SEARCH_SLOW_LOGS`, `ES_APPLICATION_LOGS`, `INDEX_SLOW_LOGS`, `AUDIT_LOGS`, a seconda dei tipi di log che desideri pubblicare. Ogni chiave deve avere un valore `LogPublishingOption` valido.

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elasticsearch-node-to-node-encryption-check

Controlla se i nodi OpenSearch Service (precedentemente chiamati Elasticsearch) sono crittografati dall'inizio alla fine. La regola è NON_COMPLIANT se la node-to-node crittografia non è abilitata nel dominio.

Identificatore: ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Tipi di risorse: AWS::Elasticsearch::Domain

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
```

```
    "NodeToNodeEncryptionOptions": BOOLEAN
}
...
```

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elastic-beanstalk-logs-to-cloudwatch

Verifica se gli ambienti AWS Elastic Beanstalk sono configurati per inviare log ad Amazon Logs. CloudWatch La regola è NON_COMPLIANT se il valore di `` è falso. StreamLogs

Identificatore: ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH

Tipi di risorse: AWS::ElasticBeanstalk::Environment

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

RetentionInDays (Facoltativo), ▪Tipo: stringa

Verifica il numero di giorni in cui conservare i log eventi prima della scadenza. I valori validi sono 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827 e 3653. La regola è NON_COMPLIANT se il valore di `logs. RetentionInDays` non corrisponde a questo parametro.

DeleteOnTerminate (Facoltativo), ▪Tipo: stringa

Verifica se i log sono configurati per essere eliminati alla cessazione dell'ambiente. I valori validi sono "true" o "false". La regola è NON_COMPLIANT se il valore di `logs. DeleteOnTerminate` non corrisponde a questo parametro.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elastic-beanstalk-managed-updates-enabled

Verifica se gli aggiornamenti gestiti della piattaforma in un ambiente sono abilitati. AWS Elastic Beanstalk La regola è CONFORME se il valore di `ManagedActionsEnabled` è impostato su true. La regola è NON_COMPLIANT se il valore di `ManagedActionsEnabled` è impostato su false o se viene fornito un parametro il cui valore non corrisponde alle configurazioni esistenti.

Identificatore: ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

Tipi di risorse: AWS::ElasticBeanstalk::Environment

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

UpdateLevel (Facoltativo), ▪Tipo: stringa

> Indica se i livelli di aggiornamento sono impostati sugli aggiornamenti delle versioni secondarie o sugli aggiornamenti della versione di patch.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

elbv2-acm-certificate-required

Verifica se Application Load Balancer e Network Load Balancer dispongono di listener configurati per utilizzare i certificati di (ACM). AWS Certificate Manager Questa regola è NON_COMPLIANT se almeno 1 sistema di bilanciamento del carico ha almeno 1 ascoltatore configurato senza un certificato ACM o configurato con un certificato diverso da un certificato ACM.

Identificatore: ELBV2_ACM_CERTIFICATE_REQUIRED

Tipi di risorse: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

AcmCertificatesAllowed (Facoltativo), Tipo: CSV

Elenco separato da virgole dei nomi della risorsa Amazon (ARN) del certificato.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elbv2-multiple-az

Verifica se un Elastic Load Balancer V2 (Application, Network, o Gateway Load Balancer) è mappato su più zone di disponibilità (AZ). La regola è NON_COMPLIANT se un Elastic Load Balancer V2 è mappato su meno di 2 AZ. Per ulteriori informazioni, consulta Zone di disponibilità per l'Application Load Balancer.

Identificatore: ELBV2_MULTIPLE_AZ

Tipi di risorse: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

minAvailabilityZones (Facoltativo), Tipo: int

Numero minimo di AZ previste (tra 2 e 10 inclusi).

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elb-acm-certificate-required

Verifica se i Classic Load Balancer utilizzano i certificati SSL forniti da. AWS Certificate Manager Per usare questa regola, devi utilizzare un listener SSL o HTTPS con il Classic Load Balancer. Questa

regola è applicabile solo ai Classic Load Balancer. Questa regola non verifica Application Load Balancer e Network Load Balancer.

Identificatore: ELB_ACM_CERTIFICATE_REQUIRED

Tipi di risorse: AWS::ElasticLoadBalancing::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elb-cross-zone-load-balancing-enabled

Controlla se il bilanciamento del carico tra zone è abilitato per i Classic Load Balancer. La regola è NON_COMPLIANT se per i Classic Load Balancer non è abilitato il bilanciamento del carico tra zone.

Identificatore: ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Tipi di risorse: AWS::ElasticLoadBalancing::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elb-custom-security-policy-ssl-check

Verifica se gli ascoltatori SSL del Classic Load Balancer usano una policy personalizzata. La regola è applicabile solo se sono presenti ascoltatori SSL per il Classic Load Balancer.

Identificatore: ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

Tipi di risorse: AWS::ElasticLoadBalancing::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Cifre ssl ProtocolsAnd, ➖Tipo: stringa

Elenco separato da virgole dei tipi di crittografia e protocolli.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elb-deletion-protection-enabled

Verifica se la protezione dall'eliminazione è abilitata per l'Elastic Load Balancer. La regola è NON_COMPLIANT se deletion_protection.enabled è false.

Identificatore: ELB_DELETION_PROTECTION_ENABLED

Tipi di risorse: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elb-logging-enabled

Verifica se la registrazione di log è abilitata per l'Application Load Balancer e il Classic Load Balancer. La regola è NON_COMPLIANT se `access_logs.s3.enabled` è false o non `access_logs.S3.bucket` è uguale alla BucketName s3 che hai fornito.

> **Note**
>
> La regola non si applica ai Network Load Balancer o ai Gateway Load Balancer.

Identifier (Identificatore): ELB_LOGGING_ENABLED

AWS::ElasticLoadBalancing::LoadBalancerTipi di risorse:, AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

s3 BucketNames (opzionale), Tipo: CSV

Elenco separato da virgole dei nomi dei bucket Amazon S3 per la consegna dei file di log da parte di Amazon ELB.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elb-predefined-security-policy-ssl-check

Verifica se gli ascoltatori SSL del Classic Load Balancer utilizzano una policy predefinita. La regola è NON_COMPLIANT se la policy dell'ascoltatore HTTPS/SSL del Classic Load Balancer non è uguale al valore del parametro "`predefinedPolicyName`".

Identificatore: ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

Tipi di risorse: AWS::ElasticLoadBalancing::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

predefinito PolicyName, ▬Tipo: stringa

Nome della policy predefinita.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

elb-tls-https-listeners-only

Verifica se il Classic Load Balancer è configurato con ascoltatori SSL o HTTPS. La regola è NON_COMPLIANT se un ascoltatore non è configurato con SSL o HTTPS.

- Se per il Classic Load Balancer non è configurato un ascoltatore, la regola restituisce NOT_APPLICABLE.
- La regola è COMPLIANT se gli ascoltatori del Classic Load Balancer sono configurati con SSL o HTTPS.
- La regola è NON_COMPLIANT se un ascoltatore non è configurato con SSL o HTTPS.

Identificatore: ELB_TLS_HTTPS_LISTENERS_ONLY

Tipi di risorse: AWS::ElasticLoadBalancing::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

emr-block-public-access

Verifica se le impostazioni di blocco dell'accesso pubblico sono abilitate per un account con Amazon EMR. La regola è NON_COMPLIANT se è falsa o, se BlockPublicSecurityGroupRules è vera, sono elencate in porte diverse dalla porta 22. PermittedPublicSecurityGroupRuleRanges

Identificatore: EMR_BLOCK_PUBLIC_ACCESS

Tipi di risorse: AWS::::Account

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

emr-kerberos-enabled

Verifica se Kerberos è abilitato per i cluster Amazon EMR. La regola è NON_COMPLIANT se una configurazione di sicurezza non è collegata al cluster o la configurazione di protezione non soddisfa i parametri della regola specificati.

Identificatore: EMR_KERBEROS_ENABLED

Tipi di risorse: AWS::EMR::Cluster

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

TicketLifetimeInHours (Facoltativo), Tipo: int

Periodo per il quale è valido il ticket Kerberos emesso dal KDC del cluster.

Realm (opzionale), ▬Tipo: stringa

Specifica il nome di dominio Kerberos dell'altro dominio della relazione di fiducia.

Domain (opzionale), ▬Tipo: stringa

Il nome di dominio dell'altro dominio della relazione di fiducia.

AdminServer (Opzionale), ▬Tipo: stringa

Specifica il nome di dominio completo del server di amministrazione nell'altro dominio della relazione di fiducia.

KdcServer (Opzionale), ▬Tipo: stringa

Il nome di dominio completo del server KDC nell'altro dominio della relazione di fiducia.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

emr-master-no-public-ip

Verifica se i nodi principali dei cluster Amazon EMR dispongono di IP pubblici. La regola è NON_COMPLIANT se il nodo master ha un IP pubblico.

> **Note**
>
> Questa regola controlla i cluster in stato RUNNING o WAITING. Questa regola richiede di abilitare la registrazione di logo per il tipo di risorsa `AWS::EC2::Instance` per avere una valutazione accurata.

Identificatore: EMR_MASTER_NO_PUBLIC_IP

Tipi di risorse: AWS::EMR::Cluster, AWS::EC2::Instance

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

encrypted-volumes

Verifica se i volumi Amazon EBS collegati sono crittografati e se sono (facoltativamente) crittografati con una chiave KMS specificata. La regola è NON_COMPLIANT se i volumi EBS collegati non sono crittografati o se sono crittografati con una chiave KMS non inclusa nei parametri forniti.

Identificatore: ENCRYPTED_VOLUMES

Tipi di risorse: AWS::EC2::Volume

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsId (opzionale), ▪Tipo: stringa

ID o ARN della chiave KMS usata per crittografare il volume.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

fms-shield-resource-policy-check

Verifica se Application Load Balancer, Amazon CloudFront distributions, Elastic Load Balancer o Elastic IP dispongono della protezione Shield. AWS Verifica inoltre se hanno un ACL web associato per le distribuzioni Application Load Balancer e Amazon CloudFront .

Identificatore: FMS_SHIELD_RESOURCE_POLICY_CHECK

Tipi di risorse: AWS::CloudFront::Distribution, AWS::ElasticLoad BalancingV2::, Balancing::,, LoadBalancer AWS::WAFRegional::WebACL, AWS::EC2::EIP, AWS::ElasticLoad LoadBalancer AWS::ShieldRegional::Protection AWS::Shield::Protection

Tipo di trigger: Modifiche alla configurazione

Regione AWS AWS : Tutte le regioni supportate

Parametri:

webACLId, ▬Tipo: stringa

WebACLId dell'ACL Web.

resourceTypes, ▬Tipo: stringa

L'ambito delle risorse a cui verrà applicata questa regola di configurazione.

resourceTags (opzionale), ▬Tipo: stringa

I tag delle risorse a cui deve essere associata la regola (ad esempio { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }).

excludeResourceTags (Facoltativo), Tipo: booleano

Se "true", esclude le risorse che corrispondono a resourceTags. Se false, include tutte le risorse che corrispondono a resourceTags.

fmsManagedToken (Opzionale), ▬Tipo: stringa

Un token generato da AWS Firewall Manager durante la creazione della regola nel tuo account. AWS Config ignora questo parametro quando si crea questa regola.

fmsRemediationEnabled (Facoltativo), Tipo: booleano

Se impostato su true, AWS Firewall Manager aggiornerà le risorse NON_COMPLIANT in base alla policy FMS. AWS Config ignora questo parametro quando si crea questa regola.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

fms-webacl-resource-policy-check

Verifica se l'ACL Web è associato a un Application Load Balancer, a una fase API Gateway o a distribuzioni Amazon CloudFront . Quando AWS Firewall Manager crea questa regola, il proprietario della policy FMS la specifica `WebACLId` nella policy FMS e può facoltativamente abilitare la correzione.

Identificatore: FMS_WEBACL_RESOURCE_POLICY_CHECK

Tipi di risorse:: AWS::CloudFront::Distribution, AWS::ApiGateway :Stage, ACL AWS::ElasticLoadBalancingV2::LoadBalancer AWS::WAFRegional::Web

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

webACLId, ▬Tipo: stringa

WebACLId dell'ACL Web.

resourceTags (opzionale), ▬Tipo: stringa

I tag delle risorse (ApplicationLoadBalancer ApiGatewayStage e CloudFront distribuzioni) a cui deve essere associata la regola. (ad esempio, {«tagKey1": [" tagValue1"], «tagKey2": [" tagValue2", «tagValue3"]})

excludeResourceTags (Facoltativo), Tipo: booleano

Se true, esclude le risorse che corrispondono a resourceTags.

fmsManagedToken (Opzionale), ▬Tipo: stringa

Un token generato da AWS Firewall Manager durante la creazione della regola nell'account del cliente. AWS Config ignora questo parametro quando il cliente crea questa regola.

fmsRemediationEnabled (Facoltativo), Tipo: booleano

Se impostato su true, AWS Firewall Manager aggiornerà le risorse non conformi in base alla policy FMS. AWS Config ignora questo parametro quando il cliente crea questa regola.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

fms-webacl-rulegroup-association-check

Verifica se i gruppi di regole sono associati all'ACL Web con la priorità corretta. La corretta priorità viene decisa dalla classificazione dei gruppi di regole nel parametro ruleGroups. Quando AWS Firewall Manager crea questa regola, assegna la massima priorità 0 seguita da 1, 2 e così via. Il proprietario della policy FMS specifica la classificazione di `ruleGroups` nella policy FMS e può facoltativamente abilitare il processo di correzione.

Identificatore: FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

Tipi di risorse: AWS::WAF::Web ACL, ACL AWS::WAFRegional::Web

Tipo di trigger: Modifiche alla configurazione

Regione AWS: tutte le regioni supportate AWS

Parametri:

ruleGroups, ▬Tipo: stringa

Elenco di coppie separate da virgole. RuleGroupIds WafOverrideAction (ad esempio, ruleGroupId -1:NONE, 2:COUNT) ruleGroupId

fmsManagedToken (Facoltativo), ▬Tipo: stringa

Un token generato da AWS Firewall Manager durante la creazione della regola nell'account del cliente. AWS Config ignora questo parametro quando il cliente crea questa regola.

fmsRemediationEnabled (Facoltativo), Tipo: booleano

Se impostato su true, AWS Firewall Manager aggiornerà le risorse non conformi in base alla policy FMS. AWS Config ignora questo parametro quando il cliente crea questa regola.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

fsx-last-backup-recovery-point-created

Verifica se è stato creato un punto di ripristino per i file system Amazon FSx. La regola è NON_COMPLIANT se il file system Amazon FSx non dispone di un punto di ripristino corrispondente creato entro il periodo di tempo specificato.

Identificatore: FSX_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipi di risorse: AWS::FSx::FileSystem

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▬Tipo: stringa

Tag dei file system Amazon FSx che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▬Tipo: stringa

ID del file system Amazon FSx che la regola deve verificare.

ripristino PointAgeValue (opzionale), Tipo: int, Impostazione predefinita: 1

Valore numerico per la durata massima consentita. Non superiore a 744 per le ore e 31 per i giorni.

ripristino PointAgeUnit (opzionale), ▬Tipo: stringa, Impostazione predefinita: giorni

Unità di tempo per la durata massima consentita. Valori accettati: "ore", "giorni".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

fsx-lustre-copy-tags-to-backups

Verifica se i file system Amazon FSx per Lustre sono configurati per copiare i tag nei backup. La regola è NON_COMPLIANT se i file system Lustre non sono configurati per copiare i tag nei backup.

Identificatore: FSX_LUSTRE_COPY_TAGS_TO_BACKUPS

Tipi di risorse: AWS::FSx::FileSystem

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

fsx-meets-restore-time-target

Verifica se il tempo di ripristino di Amazon FSx File Systems soddisfa la durata specificata. La regola è NON_COMPLIANT se un file system LatestRestoreExecutionTimeMinutes Amazon FSx dura più di minuti. maxRestoreTime

Identificatore: FSX_MEETS_RESTORE_TIME_TARGET

Tipi di risorse: AWS::FSx::FileSystem

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

max RestoreTime, Tipo: int

Valore numerico per il runtime massimo di ripristino consentito.

resourceTags (opzionale), ▬Tipo: stringa

Tag dei file system Amazon FSx che la regola deve verificare, in formato JSON.

resourceId (opzionale), ▬Tipo: stringa

ID del file system Amazon FSx che la regola deve verificare.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

fsx-openzfs-copy-tags-enabled

Verifica se i file system Amazon FSx per OpenZFS sono configurati per copiare i tag nei backup e nei volumi. La regola è NON_COMPLIANT se i file system FSx per OpenZFS non sono configurati per copiare i tag nei backup e nei volumi.

Identificatore: FSX_OPENZFS_COPY_TAGS_ENABLED

Tipi di risorse: AWS::FSx::FileSystem

Tipo di trigger: Periodico

Regione AWS: disponibile soltanto nelle regioni Europa (Stoccolma), Asia Pacifico (Mumbai), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Asia Pacifico (Hong Kong), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Europa (Londra), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Centrale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

fsx-resources-protected-by-backup-plan

Verifica se i file system Amazon FSx sono protetti da un piano di backup. La regola è NON_COMPLIANT se il file system Amazon FSx non è coperto da un piano di backup.

Identificatore: FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipi di risorse: AWS::FSx::FileSystem

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▬Tipo: stringa

Tag dei file system Amazon FSx che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▬Tipo: stringa

ID del file system Amazon FSx che la regola deve verificare.

crossRegionList (Facoltativo), ▬Tipo: stringa

Elenco separato da virgole delle regioni di destinazione della copia di backup tra regioni da conservare

crossAccountList (Opzionale), ▬Tipo: stringa

Elenco separato da virgole degli account di destinazione della copia di backup tra account da conservare

maxRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione massimo in giorni per Vault Lock di Backup

minRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione minimo in giorni per Vault Lock di Backup

backup VaultLockCheck (opzionale), ▬Tipo: stringa

Valori accettati: "True" o "False". Immetti "True" per fare in modo che la regola verifichi se per la risorsa viene eseguito il backup in un vault bloccato

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

fsx-windows-audit-log-configured

Verifica se l'audit degli accessi ai file è abilitato per i file system Amazon FSx per Windows File Server. La regola è NON_COMPLIANT se l'audit degli accessi ai file non è abilitato per i file system FSx per Windows File Server.

Identificatore: FSX_WINDOWS_AUDIT_LOG_CONFIGURED

Tipi di risorse: AWS::FSx::FileSystem

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

global-endpoint-event-replication-enabled

Verifica se la replica degli eventi è abilitata per gli endpoint EventBridge globali di Amazon. La regola è NON_COMPLIANT se la replica degli eventi non è abilitata.

Identificatore: GLOBAL_ENDPOINT_EVENT_REPLICATION_ENABLED

Tipi di risorse: AWS::Events::Endpoint

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Disponibile solo in Europa (Stoccolma), Asia Pacifico (Mumbai), Europa (Parigi), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Seoul), Asia Pacifico (Osaka), Europa (Londra), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), Asia Regione del Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Centrale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

abilitato al controllo di protezione guardduty-eks

Verifica se Audit Log Monitoring for Amazon Elastic Kubernetes Service (Amazon EKS) è abilitato per un rilevatore GuardDuty Amazon nel tuo account. La regola è NON_COMPLIANT se la funzionalità EKS Audit Log Monitoring non è abilitata per il tuo account.

Identificatore: GUARDDUTY_EKS_PROTECTION_AUDIT_ENABLED

Tipi di risorse: AWS::GuardDuty::Detector

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

abilitato per guardduty-eks-protection-runtime

Verifica se Amazon EKS Runtime Monitoring con gestione automatizzata degli agenti è abilitato per il GuardDuty rilevatore nel tuo account. La regola è NON_COMPLIANT se EKS Runtime Monitoring con gestione automatica degli agenti non GuardDuty è abilitato per il tuo account.

Identificatore: GUARDDUTY_EKS_PROTECTION_RUNTIME_ENABLED

Tipi di risorse: AWS::GuardDuty::Detector

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

guardduty-enabled-centralized

Verifica se Amazon GuardDuty è abilitato nel tuo AWS account e AWS nella tua regione. Se fornisci un AWS account per la centralizzazione, la regola valuta i GuardDuty risultati nell'account centralizzato. La regola è CONFORME quando è abilitata. GuardDuty

Identificatore: GUARDDUTY_ENABLED_CENTRALIZED

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

CentralMonitoringAccount (Facoltativo), ▬Tipo: stringa

> Elenco separato da virgole di AWS account (12 cifre) in cui è possibile GuardDuty centralizzare i risultati di Amazon.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

abilitato alla protezione lambda guardduty

Verifica se Lambda Protection è abilitata per un GuardDuty rilevatore Amazon nel tuo account. La regola è NON_COMPLIANT se la funzionalità Lambda Protection in GuardDuty Amazon non è abilitata per il tuo account.

Identificatore: GUARDDUTY_LAMBDA_PROTECTION_ENABLED

Tipi di risorse: AWS::GuardDuty::Detector

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

guardduty - abilitato alla protezione da malware

Verifica se la protezione da malware è abilitata per un GuardDuty rilevatore Amazon nel tuo account. La regola è NON_COMPLIANT se la funzionalità Malware Protection in Amazon non GuardDuty è abilitata per il tuo account.

Identificatore: GUARDDUTY_MALWARE_PROTECTION_ENABLED

Tipi di risorse: AWS::GuardDuty::Detector

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

guardduty-non-archived-findings

Verifica se Amazon GuardDuty ha risultati che non sono archiviati. La regola è NON_COMPLIANT se GuardDuty i risultati non archiviati di bassa/media/alta gravità sono più vecchi del numero specificato nel parametro /days /. daysLowSev MediumSev `daysHighSev`

Identificatore: GUARDDUTY_NON_ARCHIVED_FINDINGS

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

daysLowSev (Facoltativo), Tipo: int, Impostazione predefinita: 30

Il numero di giorni in cui i risultati di Amazon a GuardDuty bassa gravità possono rimanere non archiviati. L'impostazione di default è 30 giorni.

daysMediumSev (Facoltativo), Tipo: int, Impostazione predefinita: 7

Il numero di giorni in cui i risultati di GuardDuty media gravità di Amazon possono rimanere non archiviati. L'impostazione di default è 7 giorni.

daysHighSev (Facoltativo), Tipo: int, Impostazione predefinita: 1

Il numero di giorni in cui i risultati GuardDuty ad alta gravità di Amazon possono rimanere non archiviati. Il valore di default è 1 giorno.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

abilitato alla protezione guardduty-rds

Verifica se la protezione Amazon Relational Database Service (Amazon RDS) è abilitata per un rilevatore GuardDuty Amazon nel tuo account. La regola è NON_COMPLIANT se la funzionalità di protezione Amazon RDS in Amazon non GuardDuty è abilitata per il tuo account.

Identificatore: GUARDDUTY_RDS_PROTECTION_ENABLED

Tipi di risorse: AWS::GuardDuty::Detector

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

abilitato alla protezione guardduty-s3

Verifica se S3 Protection è abilitato per un Amazon GuardDuty Detector nel tuo account. La regola è NON_COMPLIANT se la funzionalità S3 Protection in Amazon non GuardDuty è abilitata per il tuo account.

Identificatore: GUARDDUTY_S3_PROTECTION_ENABLED

Tipi di risorse: AWS::GuardDuty::Detector

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-customer-policy-blocked-kms-actions

Verifica se le policy gestite di AWS Identity and Access Management (IAM) create non consentono azioni bloccate AWS sulle chiavi KMS. La regola è NON_COMPLIANT se qualsiasi azione bloccata è consentita sulle chiavi AWS KMS dalla policy IAM gestita.

> **Note**
>
> Questa regola non valuta variabili o condizioni nelle politiche IAM. Per ulteriori informazioni, consulta IAM Policy elements: Variables e IAM JSON Policy elements: Condition nella IAM User Guide.

Identificatore: IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

Tipi di risorse: AWS::IAM::Policy

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

bloccato ActionsPatterns, Tipo: CSV

Specificare un elenco separato da virgola di pattern di azione KMS bloccati. Ad esempio, puoi elencare kms:decrypt* o kms: come modelli di azione bloccati. ReEncrypt La regola è NON_COMPLIANT se la policy IAM gestita consente qualsiasi modello di azione elencato in questo parametro.

escludere (PermissionBoundaryPolicy facoltativo), Tipo: booleano

Flag booleano per escludere la valutazione delle policy IAM utilizzate come limiti delle autorizzazioni. Se impostato su "true", la regola non include i limiti delle autorizzazioni nella valutazione. Invece, tutte le policy IAM incluse nell'ambito vengono valutate quando il valore è impostato su "false". Il valore predefinito è "false".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

abilitato all'analizzatore di accesso esterno

Verifica se un IAM Access Analyzer per l'accesso esterno è attivato nel tuo account per regione. La regola è NON_COMPLIANT se non ci sono analizzatori per l'accesso esterno nella regione o se l'attributo 'status' non è impostato su 'ACTIVE'.

Identificatore: IAM_EXTERNAL_ACCESS_ANALYZER_ENABLED

Tipi di risorse: AWS::::Account

Tipo di trigger: Periodico

Regione AWS: tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-group-has-users-check

Verifica se i gruppi IAM contengono almeno un utente IAM.

Identificatore: IAM_GROUP_HAS_USERS_CHECK

Tipi di risorse: AWS::IAM::Group

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-inline-policy-blocked-kms-actions

Verifica se le politiche in linea allegate agli utenti, ai ruoli e ai gruppi IAM non consentono azioni bloccate su tutte le chiavi KMS. AWS La regola è NON_COMPLIANT se è consentita un'azione bloccata su tutte le chiavi AWS KMS in una politica in linea.

Identificatore: IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

AWS::IAM::GroupTipi AWS::IAM::Role di risorse:,, AWS::IAM::User

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

bloccato ActionsPatterns, Tipo: CSV

Elenco separato da virgole di schemi di azione KMS bloccati, ad esempio kms: *, kms:Decrypt, kms: *. ReEncrypt

RoleByManagementAccount escludere (Facoltativo), Tipo: booleano

Esclude un ruolo se è possibile assumerlo solo dall'account di gestione dell'organizzazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-no-inline-policy-check

Verifica se la funzionalità delle policy inline non è in uso. La regola è NON_COMPLIANT se un utente AWS Identity and Access Management (IAM), un ruolo IAM o un gruppo IAM ha una policy in linea.

Identificatore: IAM_NO_INLINE_POLICY_CHECK

Tipi di risorse:,, AWS::IAM::User AWS::IAM::Role AWS::IAM::Group

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-password-policy

Verifica se la politica sulla password dell'account per gli utenti di AWS Identity and Access Management (IAM) soddisfa i requisiti specificati indicati nei parametri. La regola è NON_COMPLIANT se la policy sulle password dell'account non soddisfa i requisiti specificati.

> **Important**
>
> I valori `true` e `false` per i parametri della regola fanno distinzione tra maiuscole e minuscole. Se `true` non viene fornito in lettere minuscole, verrà trattato come `false`.

> **Note**
>
> Risultato della valutazione per la politica di password IAM predefinita
> Questa regola è contrassegnata come NON_COMPLIANT quando viene utilizzata la politica di password IAM predefinita.
> Regole gestite e tipi di risorse IAM globali
> I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.
> Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.
> Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.

Identificatore: IAM_PASSWORD_POLICY

Tipo di trigger: Periodico

Regione AWS: tutte le AWS regioni supportate

Parametri:

RequireUppercaseCharacters (Facoltativo), Tipo: booleano, Impostazione predefinita: true

La password deve contenere almeno un carattere maiuscolo.

RequireLowercaseCharacters (Opzionale), Tipo: booleano, Impostazione predefinita: true

La password deve contenere almeno un carattere minuscolo.

RequireSymbols (Opzionale), Tipo: booleano, Impostazione predefinita: true

La password deve contenere almeno un simbolo.

RequireNumbers (Opzionale), Tipo: booleano, Impostazione predefinita: true

La password deve contenere almeno un numero.

MinimumPasswordLength (Opzionale), Tipo: int, Impostazione predefinita: 14

Lunghezza minima della password.

PasswordReusePrevention (Opzionale), Tipo: int, Impostazione predefinita: 24

Numero di password prima di permettere il riutilizzo.

MaxPasswordAge (Opzionale), Tipo: int, Impostazione predefinita: 90

Numero di giorni prima della scadenza della password.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere Creazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-policy-blacklisted-check

Verifica in ogni risorsa AWS Identity and Access Management (IAM) se una policy Amazon Resource Name (ARN) nel parametro di input è associata alla risorsa IAM. La regola è NON_COMPLIANT se l'ARN della policy è collegato alla risorsa IAM.

Identificatore: IAM_POLICY_BLACKLISTED_CHECK

Tipi di risorse: AWS::IAM::User,, AWS::IAM::Group AWS::IAM::Role

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

policyArns, Tipo: CSV, Predefinito: arn:aws:iam: :aws:policy/ AdministratorAccess

Elenco separato da virgole degli ARN della policy IAM che non devono essere collegati a nessuna entità IAM.

exceptionList (opzionale), Tipo: CSV

Elenco separato da virgole di tipi di risorse ed elenco di coppie di nomi di risorse. Ad esempio, users:[user1;user2], groups:[group1;group2], roles:[role1;role2;role3].

> **Note**
>
> Per l'elenco delle eccezioni, specificare il nome della risorsa e non l'ARN completo. Non valido:`arn:aws:iam::444455556666:role/Admin`. Valido:`Admin`.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-policy-in-use

Verifica se l'ARN della policy IAM è collegato a un utente IAM, a un gruppo con uno o più utenti IAM o a un ruolo IAM con una o più entità attendibili.

> **Note**
>
> Regole gestite e tipi di risorse IAM globali
> I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.
> Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.

Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.

Identificatore: IAM_POLICY_IN_USE

Tipi di risorse: AWS::IAM::Policy

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

policyARN, ▪Tipo: stringa

Un ARN della policy IAM da verificare.

policyUsageType (Facoltativo), ▪Tipo: stringa

Specifica se desideri che la policy sia collegata a un utente, a un gruppo o a un ruolo IAM. I valori validi sono IAM_USER, IAM_GROUP, IAM_ROLE o ANY. Il valore predefinito è ANY.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-policy-no-statements-with-admin-access

Verifica se le policy di AWS Identity and Access Management (IAM) create dispongono di istruzioni Allow che concedono le autorizzazioni a tutte le azioni su tutte le risorse. La regola è NON_COMPLIANT se l'istruzione della policy IAM gestita dal cliente include "Effect": "Allow" con "Action": "*" invece di "Resource": "*".

> **Note**
>
> Questa regola valuta solo le policy gestite dal cliente. Questa regola NON valuta le politiche in linea o le politiche AWS gestite. Per ulteriori informazioni sulla differenza, consulta Policy gestite e policy inline nella Guida per l'utente di IAM.

La seguente policy è NON_COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

La seguente policy è COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
}
```

Identifier (Identificatore): IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

Tipi di risorse: AWS::IAM::Policy

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

escludere PermissionBoundaryPolicy (facoltativo), Tipo: booleano

Flag booleano per escludere la valutazione delle policy IAM utilizzate come limiti delle autorizzazioni. Se impostato su "true", la regola non include i limiti delle autorizzazioni nella

valutazione. Invece, tutte le policy IAM incluse nell'ambito vengono valutate quando il valore è impostato su "false". Il valore predefinito è "false".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-policy-no-statements-with-full-access

Verifica se le policy di AWS Identity and Access Management (IAM) create concedono autorizzazioni a tutte le azioni sulle AWS singole risorse. La regola è NON_COMPLIANT se una policy IAM gestita dal cliente consente l'accesso completo ad almeno 1 servizio. AWS

Contesto: seguendo il principio del privilegio minimo, si consiglia di limitare le azioni consentite nelle politiche IAM quando si concedono le autorizzazioni ai servizi. AWS Questo approccio aiuta a garantire che si concedano solo le autorizzazioni necessarie specificando le azioni esatte richieste, evitando l'uso di caratteri jolly illimitati per un servizio, ad esempio. `ec2:*`

In alcuni casi, potresti voler consentire più azioni con un prefisso simile, ad esempio Logs and Zones. DescribeFlow DescribeAvailability In questi casi, puoi aggiungere un carattere jolly con suffisso al prefisso comune (ad esempio,). `ec2:Describe*` Il raggruppamento delle azioni correlate può aiutare a evitare di raggiungere i limiti di dimensione delle policy IAM.

Questa regola restituirà COMPLIANT se utilizzi azioni prefisse con un carattere jolly suffisso (ad esempio,). `ec2:Describe*` Questa regola restituirà NON_COMPLIANT solo se si utilizzano caratteri jolly senza restrizioni (ad esempio,). `ec2:*`

> **Note**
>
> Questa regola valuta solo le policy gestite dal cliente. Questa regola NON valuta le politiche in linea o le politiche gestite. AWS Per ulteriori informazioni sulla differenza, consulta Policy gestite e policy inline nella Guida per l'utente di IAM.

Identificatore: IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

Tipi di risorse: AWS::IAM::Policy

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

escludere PermissionBoundaryPolicy (facoltativo), Tipo: booleano

> Flag booleano per escludere la valutazione delle policy IAM utilizzate come limiti delle autorizzazioni. Se impostato su "true", la regola non include i limiti delle autorizzazioni nella valutazione. Invece, tutte le policy IAM incluse nell'ambito vengono valutate quando il valore è impostato su "false". Il valore predefinito è "false".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-role-managed-policy-check

Verifica se tutte le politiche gestite specificate nell'elenco delle politiche gestite sono associate al ruolo AWS Identity and Access Management (IAM). La regola è NON_COMPLIANT se una policy gestita non è collegata al ruolo IAM.

Identifier (Identificatore): IAM_ROLE_MANAGED_POLICY_CHECK

Tipi di risorse: AWS::IAM::Role

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

gestita PolicyArns, Tipo: CSV

> Elenco separato da virgole di Amazon Resource Names (ARNs) di AWS policy gestite. Per ulteriori informazioni, consulta Nomi della risorsa Amazon (ARN) e Policy gestite da AWS nella Guida per l'utente di IAM.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-root-access-key-check

Verifica se la chiave di accesso dell'utente root è disponibile. La regola è COMPLIANT se la chiave di accesso utente non esiste. Altrimenti, è NON_COMPLIANT.

> **Note**
>
> Regole gestite e tipi di risorse IAM globali
> I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.
> Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.
> Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.

Identifier (Identificatore): IAM_ROOT_ACCESS_KEY_CHECK

Tipo di trigger: Periodico

Regione AWS: tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

controllo della scadenza del certificato iam-server

Verifica se i certificati del server AWS IAM SSL/TLS archiviati in IAM sono scaduti. La regola è NON_COMPLIANT se un certificato del server IAM è scaduto.

Identificatore: IAM_SERVER_CERTIFICATE_EXPIRATION_CHECK

Tipi di risorse: AWS::IAM::ServerCertificate

Tipo di trigger: Periodico

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

iam-user-group-membership-check

Verifica se gli utenti IAM sono membri di almeno un gruppo IAM.

Identificatore: IAM_USER_GROUP_MEMBERSHIP_CHECK

Tipi di risorse: AWS::IAM::User

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

groupNames (opzionale), ▪Tipo: stringa

Elenco separato da virgole dei gruppi IAM di cui gli utenti IAM devono essere membri.

> **Note**
>
> Questa regola non supporta i nomi di gruppi con virgole.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-user-mfa-enabled

Verifica se gli utenti di AWS Identity and Access Management (IAM) hanno abilitato l'autenticazione a più fattori (MFA). La regola è NON_COMPLIANT se l'MFA non è abilitata per almeno un utente IAM.

> **Note**
>
> Regole gestite e tipi di risorse IAM globali
> I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.
> Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.
> Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.

Identifier (Identificatore): IAM_USER_MFA_ENABLED

Tipi di risorse: AWS::IAM::User

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-user-no-policies-check

Verifica se nessuno degli utenti di AWS Identity and Access Management (IAM) dispone di policy allegate. Gli utenti IAM devono ereditare le autorizzazioni da gruppi o ruoli IAM. La regola è NON_COMPLIANT se esiste almeno un utente IAM con policy collegate.

Identificatore: IAM_USER_NO_POLICIES_CHECK

Tipi di risorse: AWS::IAM::User

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

iam-user-unused-credentials-check

Verifica se i tuoi utenti AWS Identity and Access Management (IAM) dispongono di password o chiavi di accesso attive che non sono state utilizzate entro il numero di giorni specificato che hai fornito. La regola è NON_COMPLIANT se ci sono account inattivi non utilizzati di recente.

> **Note**
>
> Cronologia della rivalutazione
> Rivalutare questa regola entro 4 ore dalla prima valutazione non avrà effetto sui risultati.
> Regole gestite e tipi di risorse IAM globali
> I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022.

Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.
Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.
Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.

Identifier (Identificatore): IAM_USER_UNUSED_CREDENTIALS_CHECK

Tipi di risorse: AWS::IAM::User

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

CredentialUsageEtà massima, Tipo: int, Impostazione predefinita: 90

Numero massimo di giorni in cui le credenziali non possono essere utilizzate. Il valore predefinito è 90 giorni.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

restricted-ssh

Important

Per questa regola, l'identificatore (INCOMING_SSH_DISABLED) e il nome della regola (restricted-ssh) sono diversi.

Verifica se il traffico SSH in entrata per i gruppi di sicurezza risulta accessibile. La regola è COMPLIANT quando gli indirizzi IP del traffico SSH in entrata nei gruppi di sicurezza hanno restrizioni (CIDR diverso da 0.0.0.0/0 o ::/0). Altrimenti, è NON_COMPLIANT.

Identificatore: INCOMING_SSH_DISABLED

Tipi di risorse: AWS::EC2::SecurityGroup

Tipo di trigger: Modifiche alla configurazione e periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

abilitato a inspector-ec2-scan

Verifica se la scansione di Amazon Inspector V2 EC2 è attivata per il tuo ambiente con account singolo o multiplo per rilevare potenziali vulnerabilità e problemi di raggiungibilità della rete sulle tue istanze EC2. La regola è NON_COMPLIANT se la scansione EC2 non è attivata.

Identificatore: INSPECTOR_EC2_SCAN_ENABLED

Tipi di risorse: AWS::::Account

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

abilitato a Inspector-ecr-scan

Verifica se la scansione ECR di Amazon Inspector V2 è attivata per il tuo ambiente con account singolo o multiplo per rilevare potenziali vulnerabilità del software nelle immagini dei container. La regola è NON_COMPLIANT se la scansione ECR non è attivata.

Identificatore: INSPECTOR_ECR_SCAN_ENABLED

Tipi di risorse: AWS::::Account

Tipo di trigger: Periodico

Regione AWS: tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

abilitato alla scansione del codice lambda dell'ispettore

Verifica se la scansione del codice Lambda di Amazon Inspector V2 è attivata per il tuo ambiente con account singolo o multiplo per rilevare potenziali vulnerabilità del codice. La regola è NON_COMPLIANT se la scansione del codice Lambda non è attivata.

Identificatore: INSPECTOR_LAMBDA_CODE_SCAN_ENABLED

Tipi di risorse: AWS::::Account

Tipo di trigger: Periodico

Regione AWS: Disponibile solo nelle regioni Europa (Stoccolma), Stati Uniti orientali (Ohio), Europa (Irlanda), Europa (Francoforte), Stati Uniti orientali (Virginia settentrionale), Europa (Londra), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Asia Pacifico (Singapore), Asia Pacifico (Sydney)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

inspector-lambda-standard-scan abilitato

Verifica se la scansione standard di Amazon Inspector V2 Lambda è attivata per il tuo ambiente con account singolo o multiplo per rilevare potenziali vulnerabilità del software. La regola è NON_COMPLIANT se la scansione standard Lambda non è attivata.

Identificatore: INSPECTOR_LAMBDA_STANDARD_SCAN_ENABLED

Tipi di risorse: AWS::::Account

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ec2-instances-in-vpc

> **Important**
>
> Per questa regola, l'identificatore (INSTANCES_IN_VPC) e il nome della regola (ec2-instances-in-vpc) sono diversi.

Verifica se le istanze EC2 appartengono a un cloud privato virtuale (VPC). Facoltativamente, puoi specificare l'ID VPC da associare alle istanze.

Identificatore: INSTANCES_IN_VPC

Tipi di risorse: AWS::EC2::Instance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

vpcId (opzionale), ▪Tipo: stringa

L'ID del VPC contenente queste istanze EC2.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

internet-gateway-authorized-vpc-only

Verifica se i gateway Internet sono collegati a un cloud privato virtuale (Amazon VPC) autorizzato. La regola è NON_COMPLIANT se i gateway Internet sono collegati a un VPC non autorizzato.

Identificatore: INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY

Tipi di risorse: AWS::EC2::InternetGateway

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

AuthorizedVpcIds (Facoltativo), ▪Tipo: stringa

Elenco separato da virgole degli ID VPC autorizzati con IGW associati. Se il parametro non viene fornito, tutti gli IGW collegati saranno NON_COMPLIANT.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

kinesis-firehose-delivery-stream-criptato

Verifica se i flussi di distribuzione di Amazon Kinesis Data Firehose sono crittografati quando sono inattivi con crittografia lato server. La regola è NON_COMPLIANT se un flusso di distribuzione di Kinesis Data Firehose non è crittografato quando è inattivo con la crittografia lato server.

Identificatore: KINESIS_FIREHOSE_DELIVERY_STREAM_ENCRYPTED

Tipi di risorse: AWS::KinesisFirehose::DeliveryStream

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsKeyArns (Facoltativo), Tipo: CSV

Elenco separato da virgole di Key Arn KMS approvati per l'utilizzo di Kinesis Firehose.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

kinesis-stream-encrypted

Verifica se i flussi Amazon Kinesis sono crittografati a riposo con crittografia lato server. La regola è NON_COMPLIANT per uno stream Kinesis se '' non è presente. StreamEncryption

Contesto: la crittografia lato server è una funzionalità di Amazon Kinesis Data Streams che crittografa automaticamente i dati prima che siano inattivi utilizzando una chiave KMS. AWS I dati vengono crittografati prima di essere scritti sul livello di archiviazione del flusso Kinesis e vengono decrittografati dopo essere stati recuperati dall'archiviazione. Di conseguenza, i dati vengono sempre crittografati mentre sono inattivi all'interno del servizio del flusso di dati Kinesis. In questo modo potrai soddisfare i requisiti normativi e migliorare la sicurezza dei dati. Per ulteriori informazioni, consulta Protezione dei dati in Flusso di dati Amazon Kinesis.

Identificatore: KINESIS_STREAM_ENCRYPTED

Tipi di risorse: AWS::Kinesis::Stream

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

kms-cmk-not-scheduled-for-deletion

Verifica se le AWS chiavi del Key Management Service (AWS KMS) non sono pianificate per l'eliminazione in KMS. AWS La regola è NON_COMPLIANT se è pianificata l'eliminazione delle chiavi KMS.

Identificatore: KMS_CMK_NOT_SCHEDULED_FOR_DELETION

Tipi di risorse: AWS::KMS::Key

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsKeyIds (Facoltativo), ▬Tipo: stringa

(Opzionale) Elenco separato da virgole di specifici ID chiave gestiti dal cliente da non pianificare per l'eliminazione. Se non si specifica alcuna chiave, la regola controlla tutte le chiavi.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

lambda-concurrency-check

Verifica se la funzione Lambda è configurata con un limite di esecuzioni simultanee a livello di funzione. La regola è NON_COMPLIANT se la funzione Lambda non è configurata con un limite di esecuzioni simultanee a livello di funzione.

Identificatore: LAMBDA_CONCURRENCY_CHECK

Tipi di risorse: AWS::Lambda::Function

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

ConcurrencyLimitLow (Facoltativo), ▪Tipo: stringa

Limite minimo di esecuzioni simultanee

ConcurrencyLimitHigh (Opzionale), ▪Tipo: stringa

Limite massimo di esecuzioni simultanee

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

lambda-dlq-check

Verifica se una funzione Lambda è configurata con una coda DLQ. La regola è NON_COMPLIANT se la funzione Lambda non è configurata con una coda DLQ.

Identificatore: LAMBDA_DLQ_CHECK

Tipi di risorse: AWS::Lambda::Function

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

dlqArns (opzionale), ▪Tipo: stringa

Elenco separato da virgole degli ARN Amazon SQS e Amazon SNS che devono essere configurati come destinazione della coda DLQ della funzione Lambda.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

lambda-function-public-access-prohibited

Verifica se la politica della AWS Lambda funzione allegata alla risorsa Lambda proibisce l'accesso pubblico. Se la policy della funzione Lambda consente l'accesso pubblico, è NON_COMPLIANT.

Contesto: si ritiene che una policy della funzione lambda consenta l'accesso pubblico se l'elemento principale è vuoto o contiene un carattere jolly. Ad esempio, se l'elemento principale è `“”` o. `{“AWS”: “”}` La concessione dell'accesso pubblico non è consigliata per motivi di sicurezza. Limitare l'accesso pubblico può aiutarti a prevenire le chiamate non autorizzate delle funzioni Lambda, che potrebbero compromettere i dati o comportare costi indesiderati.

Per limitare l'accesso alle funzioni Lambda, specifica gli ID AWS account o gli Amazon Resource Names (ARN) degli utenti, dei ruoli o dei servizi IAM che possono richiamare le funzioni. Per ulteriori informazioni, consulta Concedere l'accesso alla funzione ad altri account nella Guida per gli sviluppatori.AWS Lambda

Identificatore: LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED

Tipi di risorse: AWS::Lambda::Function

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

lambda-function-settings-check

Verifica se le impostazioni della funzione AWS Lambda per runtime, ruolo, timeout e dimensione della memoria corrispondono ai valori previsti. La regola ignora le funzioni con il tipo di pacchetto

'Image' e le funzioni con runtime impostato su 'OS-only Runtime'. La regola è NON_COMPLIANT se le impostazioni della funzione Lambda non corrispondono ai valori previsti.

Identificatore: LAMBDA_FUNCTION_SETTINGS_CHECK

Tipi di risorse: AWS::Lambda::Function

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

runtime, Tipo: CSV

Elenco separato da virgole di valori di runtime AWS Lambda

role (opzionale), ▬Tipo: stringa

Nome o ARN del ruolo di esecuzione Lambda AWS

timeout (opzionale), Tipo: int, Impostazione predefinita: 3

AWS Timeout della funzione Lambda in secondi

memorySize (opzionale), Tipo: int, Impostazione predefinita: 128

AWS Dimensione della funzione Lambda in megabyte

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with Rules. AWS Config Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
    "MemorySize": Integer*,
    "Role": String*,
    "Runtime": String*,
    "Timeout": Integer*
}
...
```

* Per ulteriori informazioni sui valori validi per questi input, vedere Role MemorySize, Runtime e Timeout nella Guida per l'utente. AWS CloudFormation

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

lambda-inside-vpc

Verifica se a una funzione Lambda è consentito l'accesso a un cloud privato virtuale (VPC). La regola è NON_COMPLIANT se la funzione Lambda non è abilitata per il VPC.

Identificatore: LAMBDA_INSIDE_VPC

Tipi di risorse: AWS::Lambda::Function

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

subnetIds (opzionale), ▬Tipo: stringa

Elenco separato da virgole degli ID di sottoreti a cui possono essere associate le funzioni Lambda.

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
   "VpcConfig": {
         "SubnetIds": "[SubnetId-1, SubnetId-2, SubnetId-3, ...]"
```

```
    }
}
...
```

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

lambda-vpc-multi-az-check

Verifica se a Lambda è associata più di 1 zona di disponibilità. La regola è NON_COMPLIANT se a Lambda è associata solo 1 zona di disponibilità o se il numero di zone di disponibilità associate è inferiore al numero specificato nel parametro opzionale.

Identificatore: LAMBDA_VPC_MULTI_AZ_CHECK

Tipi di risorse: AWS::Lambda::Function

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

availabilityZones (opzionale), Tipo: int

Numero di zone di disponibilità previste.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

macie-auto-sensitive-data-discovery-check

Verifica se il rilevamento automatico dei dati sensibili è abilitato per Amazon Macie. La regola è NON_COMPLIANT se il rilevamento automatico dei dati sensibili è disabilitato. La regola è APPLICABILE per gli account amministratore e NOT_APPLICABLE per gli account membro.

Identificatore: MACIE_AUTO_SENSITIVE_DATA_DISCOVERY_CHECK

Tipi di risorse: AWS::::Account

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

macie-status-check

Verifica se Amazon Macie è abilitato nell'account in base alla regione. La regola è NON_COMPLIANT se l'attributo "status" non è impostato su "ENABLED".

Identificatore: MACIE_STATUS_CHECK

Tipi di risorse: AWS::::Account

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

mfa-enabled-for-iam-console-access

Verifica se l' AWS autenticazione a più fattori (MFA) è abilitata per AWS tutti gli utenti di Identity and Access Management (IAM) che utilizzano una password della console. La regola è COMPLIANT quando MFA è abilitata.

> **Note**
>
> Cronologia della rivalutazione
>
> Rivalutare questa regola entro 4 ore dalla prima valutazione non avrà effetto sui risultati.
>
> Regole gestite e tipi di risorse IAM globali
>
> I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`AWS::IAM::Role, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.
>
> Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.
>
> Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.

Identifier (Identificatore): MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

Tipi di risorse: AWS::IAM::User

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

mq-active-deployment-mode

Verifica la modalità di implementazione configurata per il motore di broker ActiveMQ di Amazon MQ. La regola è NON_COMPLIANT se è in uso la modalità broker a istanza singola predefinita.

Identificatore: MQ_ACTIVE_DEPLOYMENT_MODE

Tipi di risorse: AWS::AmazonMQ::Broker

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

mq-automatic-minor-version-upgrade-enabled

Verifica se gli aggiornamenti automatici delle versioni secondarie sono abilitati per i broker Amazon MQ. La regola è NON_COMPLIANT se il campo 'AutoMinorVersionUpgrade' non è abilitato per un broker Amazon MQ.

Identificatore: MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Tipi di risorse: AWS::AmazonMQ::Broker

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

mq-auto-minor-version-upgrade-enabled

Verifica se gli aggiornamenti automatici delle versioni secondarie sono abilitati per i broker Amazon MQ. La regola è NON_COMPLIANT se il campo 'AutoMinorVersionUpgrade' non è abilitato per un broker Amazon MQ.

Identificatore: MQ_AUTO_MINOR_VERSION_UPGRADE_ENABLED

Tipi di risorse: AWS::AmazonMQ::Broker

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

mq-cloudwatch-audit-logging-enabled

Verifica se i broker Amazon MQ hanno abilitato la registrazione CloudWatch di audit di Amazon. La regola è NON_COMPLIANT se la registrazione di log di audit non è abilitata per un broker.

Identificatore: MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED

Tipi di risorse: AWS::AmazonMQ::Broker

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

abilitato per mq-cloudwatch-audit-log

Verifica se un broker Amazon MQ ha abilitato la registrazione di CloudWatch controllo. La regola è NON_COMPLIANT se il broker non ha abilitato la registrazione di controllo.

Identificatore: MQ_CLOUDWATCH_AUDIT_LOG_ENABLED

Tipi di risorse: AWS::AmazonMQ::Broker

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

mq-no-public-access

Verifica se i broker Amazon MQ non sono accessibili pubblicamente. La regola è NON_COMPLIANT se il campo 'PubliclyAccessible' è impostato su true per un broker Amazon MQ.

Identificatore: MQ_NO_PUBLIC_ACCESS

Tipi di risorse: AWS::AmazonMQ::Broker

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

mq-rabbit-deployment-mode

Verifica la modalità di implementazione configurata per il motore di broker RabbitMQ di Amazon MQ. La regola è NON_COMPLIANT se è in uso la modalità broker a istanza singola predefinita.

Identificatore: MQ_RABBIT_DEPLOYMENT_MODE

Tipi di risorse: AWS::AmazonMQ::Broker

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

msk-enhanced-monitoring-enabled

Verifica se il monitoraggio avanzato è abilitato per un cluster Amazon MSK impostato su PER_TOPIC_PER_BROKER o PER_TOPIC_PER_PARTITION. La regola è NON_COMPLIANT se il monitoraggio avanzato è abilitato e impostato su DEFAULT o PER_BROKER.

Identificatore: MSK_ENHANCED_MONITORING_ENABLED

Tipi di risorse: AWS::MSK::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

msk-in-cluster-node-require-tls

Verifica se un cluster Amazon MSK impone la crittografia in transito utilizzando HTTPS (TLS) con i nodi broker del cluster. La regola è NON_COMPLIANT se la comunicazione in testo semplice è abilitata per le connessioni dei nodi broker all'interno del cluster.

Identificatore: MSK_IN_CLUSTER_NODE_REQUIRE_TLS

Tipi di risorse: AWS::MSK::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

multi-region-cloudtrail-enabled

> **Important**
>
> Per questa regola, l'identificatore (MULTI_REGION_CLOUD_TRAIL_ENABLED) e il nome della regola (multi-region-cloudtrail-enabled) sono diversi.

Verifica se esiste almeno una regione multipla. AWS CloudTrail La regola è NON_COMPLIANT se i trail non corrispondono ai parametri di input. La regola è NON_COMPLIANT se il `ExcludeManagementEventSources` campo non è vuoto o se AWS CloudTrail è configurato per escludere eventi di gestione come eventi AWS KMS o eventi Amazon RDS Data API.

Identifier (Identificatore): MULTI_REGION_CLOUD_TRAIL_ENABLED

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

s3 BucketName (opzionale), ▪Tipo: stringa

Nome del bucket Amazon S3 a cui inviare i file AWS CloudTrail di log.

snsTopicArn (Facoltativo), ▪Tipo: stringa

Argomento Amazon SNS ARN da utilizzare AWS CloudTrail per le notifiche.

cloud WatchLogsLogGroupArn (opzionale), ▪Tipo: stringa

ARN del gruppo di CloudWatch log Amazon a AWS CloudTrail cui inviare dati.

includeManagementEvents (Facoltativo), Tipo: booleano

Selettore di eventi per includere gli eventi di gestione per. AWS CloudTrail

readWriteType (Facoltativo), ▪Tipo: stringa

Tipo di eventi da registrare. I valori validi sono ReadOnly, WriteOnly e ALL.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

nacl-no-unrestricted-ssh-rdp

Verifica se le porte predefinite per il traffico in entrata SSH/RDP per le liste di controllo degli accessi di rete (NACL) non sono soggette a restrizioni. La regola è NON_COMPLIANT se una voce in entrata della NACL consente un blocco CIDR UDP o TCP di origine per le porte 22 o 3389.

Identificatore: NACL_NO_UNRESTRICTED_SSH_RDP

Tipi di risorse: AWS::EC2::NetworkAcl

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

neptune-cluster-backup-retention-check

Verifica se il periodo di conservazione del cluster database di Amazon Neptune è impostato su un numero di giorni specifico. La regola è NON_COMPLIANT se il periodo di conservazione è inferiore al valore specificato dal parametro.

Identificatore: NEPTUNE_CLUSTER_BACKUP_RETENTION_CHECK

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

minimo BackupRetentionPeriod (opzionale), Tipo: int

> Numero minimo di giorni in cui conservare i backup. I valori validi vanno da 1 a 35 e il valore predefinito è 7. La regola è NON_COMPLIANT se il valore è maggiore di 'backup'. RetentionPeriod La regola è CONFORME se il valore è minore o uguale a 'backup'. RetentionPeriod

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

neptune-cluster-cloudwatch-log-export-enabled

Verifica se un cluster Amazon Neptune CloudWatch ha abilitato l'esportazione dei log per i log di controllo. La regola è NON_COMPLIANT se un cluster Neptune non ha l'esportazione dei log abilitata per i log di controllo. CloudWatch

Identificatore: NEPTUNE_CLUSTER_CLOUDWATCH_LOG_EXPORT_ENABLED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: AWS Tutte le regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

neptune-cluster-copy-tags-to-snapshot-enabled

Verifica se un cluster Amazon Neptune è configurato per copiare tutti i tag negli snapshot al momento della creazione degli snapshot. La regola è NON_COMPLIANT se 'copy Snapshot' è impostato su false. TagsTo

Identificatore: NEPTUNE_CLUSTER_COPY_TAGS_TO_SNAPSHOT_ENABLED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS AWS : Tutte le regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

neptune-cluster-deletion-protection-enabled

Verifica se la protezione dall'eliminazione è abilitata nei cluster database Amazon Neptune. La regola è NON_COMPLIANT se il campo deletionProtection del cluster Amazon Neptune è impostato su false.

Identificatore: NEPTUNE_CLUSTER_DELETION_PROTECTION_ENABLED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

neptune-cluster-encrypted

Verifica se la crittografia dell'archiviazione è abilitata per i cluster database Amazon Neptune. La regola è NON_COMPLIANT se la crittografia di archiviazione non è abilitata.

Identificatore: NEPTUNE_CLUSTER_ENCRYPTED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

KmsKeyArns (Facoltativo), Tipo: CSV

Un elenco separato da virgole di ARN di chiavi KMS da confrontare con quello del KmsKeyId cluster crittografato.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

neptune-cluster-iam-database-authentication

Verifica se un cluster Amazon Neptune AWS ha l'autenticazione del database Identity and Access Management (IAM) abilitata. La regola è NON_COMPLIANT se l'autenticazione database di IAM non è abilitata per un cluster Amazon Neptune.

Identificatore: NEPTUNE_CLUSTER_IAM_DATABASE_AUTHENTICATION

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

neptune-cluster-multi-az-enabled

Verifica se un cluster Amazon Neptune è configurato con la replica Amazon RDS Multi-AZ. La regola è NON_COMPLIANT se la replica Multi-AZ non è abilitata.

Identificatore: NEPTUNE_CLUSTER_MULTI_AZ_ENABLED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

neptune-cluster-snapshot-encrypted

Verifica se un cluster database Amazon Neptune contiene snapshot crittografati. La regola è NON_COMPLIANT se un cluster Neptune non contiene snapshot crittografati.

Identificatore: NEPTUNE_CLUSTER_SNAPSHOT_ENCRYPTED

Tipi di risorse: AWS: :RDS: :DB ClusterSnapshot

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

neptune-cluster-snapshot-public-prohibited

Verifica se uno snapshot del cluster database manuale Amazon Neptune è pubblico. La regola è NON_COMPLIANT se qualsiasi snapshot del cluster Neptune nuovo ed esistente è pubblico.

Identificatore: NEPTUNE_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

Tipi di risorse: AWS: :RDS: :DB ClusterSnapshot

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

netfw-deletion-protection-enabled

Verifica se AWS Network Firewall ha la protezione da eliminazione abilitata. La regola è NON_COMPLIANT se la protezione dall'eliminazione non è abilitata per Network Firewall.

Identificatore: NETFW_DELETION_PROTECTION_ENABLED

Tipi di risorse: AWS::NetworkFirewall::Firewall

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

netfw-logging-enabled

Verifica se i firewall AWS Network Firewall hanno la registrazione abilitata. Questa regola è NON_COMPLIANT se non è configurato nessun tipo di registrazione di log. Puoi specificare il tipo di registrazione di log che desideri venga verificato dalla regola.

Identificatore: NETFW_LOGGING_ENABLED

Tipi di risorse: AWS::NetworkFirewall::LoggingConfiguration

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

logType (opzionale), ▬Tipo: stringa

logType (opzionale): tipo di log in cui la regola deve verificare la presenza dii firewall: "alert", "flow" o "both".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

netfw-multi-az-enabled

Verifica se i firewall AWS Network Firewall sono distribuiti su più zone di disponibilità. La regola è NON_COMPLIANT se i firewall sono implementati in una sola zona di disponibilità o in un numero di zone inferiore al numero indicato nel parametro opzionale.

Identificatore: NETFW_MULTI_AZ_ENABLED

Tipi di risorse: AWS::NetworkFirewall::Firewall

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

availabilityZones (opzionale), Tipo: int

Il numero di zone di disponibilità previste.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

netfw-policy-default-action-fragment-packets

Verifica se una policy AWS Network Firewall è configurata con un'azione predefinita stateless definita dall'utente per i pacchetti frammentati. La regola è NON_COMPLIANT se l'azione predefinita stateless per i pacchetti frammentati non corrisponde all'azione predefinita definita dall'utente.

Identificatore: NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS

Tipi di risorse: AWS::NetworkFirewall::FirewallPolicy

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

azioni senza stato FragmentDefault, Tipo: CSV

> Elenco di valori separati da virgole. Puoi selezionare un massimo di due valori. I valori validi includono "aws:pass", "aws:drop" e "aws:forward_to_sfe".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

netfw-policy-default-action-full-packets

Verifica se una policy AWS Network Firewall è configurata con un'azione stateless predefinita definita dall'utente per pacchetti completi. Questa regola è NON_COMPLIANT se l'azione stateless predefinita per i pacchetti completi non corrisponde all'azione stateless predefinita definita dall'utente.

Identificatore: NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS

Tipi di risorse: AWS::NetworkFirewall::FirewallPolicy

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

apolide DefaultActions, Tipo: CSV

Elenco di valori separati da virgole. Puoi selezionare un massimo di due valori. I valori validi includono "aws:pass", "aws:drop" e "aws:forward_to_sfe".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

netfw-policy-rule-group-associated

Verifica che la politica del AWS Network Firewall sia associata a gruppi di regole stateful OR stateless. Questa regola è NON_COMPLIANT se nessun gruppo di regole stateful o stateless è associato alla policy Network Firewall, altrimenti è COMPLIANT se è presente uno dei gruppi di regole.

Identificatore: NETFW_POLICY_RULE_GROUP_ASSOCIATED

Tipi di risorse: AWS::NetworkFirewall::FirewallPolicy

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

netfw-stateless-rule-group-not-empty

Verifica se un gruppo di regole Network Firewall stateless contiene regole. La regola è NON_COMPLIANT se un gruppo di regole Network Firewall stateless non contiene regole.

Identificatore: NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

Tipi di risorse: AWS::NetworkFirewall::RuleGroup

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

nlb-cross-zone-load-balancing-enabled

Verifica se sui Network Load Balancer (NLB) è abilitato il bilanciamento del carico tra zone. La regola è NON_COMPLIANT se per un NLB il bilanciamento del carico tra zone non è abilitato.

Identificatore: NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Tipi di risorse: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

no-unrestricted-route-to-igw

Verifica se sono presenti route pubbliche nella tabella di routing verso un gateway Internet (IGW). La regola è NON_COMPLIANT se una route verso un IGW dispone di un blocco CIDR di destinazione di "0.0.0.0/0" o "::/0" o se un blocco CIDR di destinazione non corrisponde al parametro della regola.

Identificatore: NO_UNRESTRICTED_ROUTE_TO_IGW

Tipi di risorse: AWS::EC2::RouteTable

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

routeTableIds (Facoltativo), Tipo: CSV

> Elenco separato da virgole degli ID delle tabelle di routing che possono avere route verso un gateway Internet con un blocco CIDR di destinazione di "0.0.0.0/0" o "::/0".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

opensearch-access-control-enabled

Verifica se nei domini Amazon OpenSearch Service è abilitato il controllo granulare degli accessi. La regola è NON_COMPLIANT se AdvancedSecurityOptions non è abilitata per il dominio Service. OpenSearch

Identificatore: OPENSEARCH_ACCESS_CONTROL_ENABLED

Tipi di risorse: AWS::OpenSearch::Domain

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

opensearch-audit-logging-enabled

Verifica se nei domini Amazon OpenSearch Service è abilitata la registrazione di controllo. La regola è NON_COMPLIANT se un dominio di OpenSearch servizio non ha la registrazione di controllo abilitata.

Identificatore: OPENSEARCH_AUDIT_LOGGING_ENABLED

Tipi di risorse: AWS::OpenSearch::Domain

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

cloud WatchLogsLogGroupArnList (opzionale), Tipo: CSV

> Elenco separato da virgole di Amazon Resource Names (ARN) per i gruppi di log Amazon CloudWatch Logs. La regola verifica se i gruppi di log specificati sono configurati per i log di controllo.
>
> I valori validi includono: `arn:aws:logs:region:account-id:log-group:log_group_name:*` e `arn:aws:logs:region:account-id:log-group:log_group_name`.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

opensearch-data-node-fault-tolerance

Verifica se i domini Amazon OpenSearch Service sono configurati con almeno tre nodi di dati e se zoneAwarenessEnabled sono veri. La regola è NON_COMPLIANT per un dominio OpenSearch se 'instanceCount' è inferiore a 3 o 'zone 'è impostato su 'false'. AwarenessEnabled

Identificatore: OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

Tipi di risorse: AWS::OpenSearch::Domain

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

opensearch-encrypted-at-rest

Verifica se nei domini Amazon OpenSearch Service è abilitata la configurazione Encryption at Rest. La regola è NON_COMPLIANT se il campo `EncryptionAtRestOptions` non è abilitato.

> **Note**
>
> La regola non valuta i domini Eslasticsearch.

Identificatore: OPENSEARCH_ENCRYPTED_AT_REST

Tipi di risorse: AWS::OpenSearch::Domain

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

opensearch-https-required

Verifica se le connessioni ai domini utilizzano HTTPS. OpenSearch La regola è NON_COMPLIANT se il dominio Amazon OpenSearch «enforceHTTPS» non è «vero» o è «vero» e «TLS» non è in «». SecurityPolicy `tlsPolicies`

Identificatore: OPENSEARCH_HTTPS_REQUIRED

Tipi di risorse: AWS::OpenSearch::Domain

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

tlsPolicies (opzionale), Tipo: CSV

> Elenco separato da virgole di politiche di sicurezza TLS da verificare rispetto al dominio Amazon. OpensSearch

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

opensearch-in-vpc-only

Verifica se i domini OpenSearch di Amazon Service si trovano in un Amazon Virtual Private Cloud (VPC). La regola è NON_COMPLIANT se un OpenSearch endpoint del dominio Service è pubblico.

> **Note**
>
> La regola non valuta i domini Eslasticsearch.

Identificatore: OPENSEARCH_IN_VPC_ONLY

Tipi di risorse: AWS::OpenSearch::Domain

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

opensearch-logs-to-cloudwatch

Verifica se i domini Amazon OpenSearch Service sono configurati per inviare log ad Amazon CloudWatch Logs. La regola è NON_COMPLIANT se la registrazione di log non è configurata.

> **Note**
>
> La regola non valuta i domini Eslasticsearch.

Identificatore: OPENSEARCH_LOGS_TO_CLOUDWATCH

Tipi di risorse: AWS::OpenSearch::Domain

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

logTypes (opzionale), Tipo: CSV

Elenco separato da virgole dei log abilitati. I valori validi sono "search", "index", "error".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

opensearch-node-to-node-encryption-check

Verifica se i nodi OpenSearch di Amazon Service sono crittografati end-to-end. La regola è NON_COMPLIANT se la node-to-node crittografia non è abilitata nel dominio

> **Note**
>
> La regola non valuta i domini Eslasticsearch.

Identificatore: OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Tipi di risorse: AWS::OpenSearch::Domain

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

opensearch-primary-node-fault-tolerance

Verifica se i domini Amazon OpenSearch Service sono configurati con almeno tre nodi primari dedicati. La regola è NON_COMPLIANT per un dominio di OpenSearch servizio se 'DedicatedMasterEnabled' è impostato su 'false' o 'Count' è inferiore a 3. DedicatedMaster

Identificatore: OPENSEARCH_PRIMARY_NODE_FAULT_TOLERANCE

Tipi di risorse: AWS::OpenSearch::Domain

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

opensearch-update-check

Verifica se gli aggiornamenti della versione di Amazon OpenSearch Service sono disponibili ma non installati. La regola è NON_COMPLIANT per un OpenSearch dominio se non sono installati gli ultimi aggiornamenti software.

Identificatore: OPENSEARCH_UPDATE_CHECK

Tipi di risorse: AWS::OpenSearch::Domain

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-aurora-mysql-audit-logging-enabled

Verifica se i cluster Edition compatibili con Amazon Aurora MySQL sono configurati per pubblicare log di controllo su Amazon Logs. CloudWatch La regola è NON_COMPLIANT se i cluster Aurora MySQL-Compatible Edition non sono abilitati per i la pubblicazione dei log.

Identificatore: RDS_AURORA_MYSQL_AUDIT_LOGGING_ENABLED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-automatic-minor-version-upgrade-enabled

Verifica se le istanze database Amazon Relational Database Service (Amazon RDS) sono configurate per gli aggiornamenti automatici delle versioni secondarie. La regola è NON_COMPLIANT se il valore di MinorVersion 'auto Upgrade' è falso.

Identificatore: RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS AWS : Tutte le regioni supportate

Parametri:

Nessuno

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
    "AutoMinorVersionUpgrade": BOOLEAN*,
    "Engine": String*
}
```

```
...
```

* Per ulteriori informazioni sui valori validi per questi input, vedere _AutoMinorVersionUpgrade and Engine nella Guida per l'utente. AWS CloudFormation

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-cluster-auto-minor-version-upgrade-enable

Verifica se gli aggiornamenti automatici delle versioni secondarie sono abilitati per le implementazioni dei cluster Amazon RDS Multi-AZ. La regola è NON_COMPLIANT se Upgrade è impostato su false. autoMinorVersion

Identificatore: RDS_CLUSTER_AUTO_MINOR_VERSION_UPGRADE_ENABLE

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-cluster-default-admin-check

Verifica se il nome utente amministratore di un cluster di database Amazon Relational Database Service (Amazon RDS) è diverso rispetto al valore predefinito. La regola è NON_COMPLIANT se il nome utente amministratore è impostato sul valore predefinito.

Identificatore: RDS_CLUSTER_DEFAULT_ADMIN_CHECK

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

valido AdminUserNames (facoltativo), Tipo: CSV

> Elenco separato da virgole dei nomi utente amministratore che i cluster Amazon RDS possono utilizzare. Non è possibile includere "postgres" o "admin" come nomi utente validi poiché si tratta di valori predefiniti.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-cluster-deletion-protection-enabled

Verifica se la protezione dall'eliminazione è abilitata per un cluster Amazon Relational Database Service (Amazon RDS). La regola è NON_COMPLIANT se la protezione dall'eliminazione non è abilitata per un cluster Amazon RDS.

Identificatore: RDS_CLUSTER_DELETION_PROTECTION_ENABLED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-cluster-encrypted-at-rest

Verifica se la crittografia a riposo è abilitata per i cluster Amazon Relational Database Service (Amazon RDS). La regola è NON_COMPLIANT se un cluster Amazon RDS non è crittografato a riposo.

Identificatore: RDS_CLUSTER_ENCRYPTED_AT_REST

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

rds-cluster-iam-authentication-enabled

Verifica se un cluster Amazon Relational Database Service (Amazon RDS) AWS ha l'autenticazione Identity and Access Management (IAM) abilitata. La regola è NON_COMPLIANT se l'autenticazione IAM non è abilitata per un cluster Amazon RDS.

Identificatore: RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-cluster-multi-az-enabled

Verifica se la replica di più zone di disponibilità (Multi-AZ) è abilitata sui cluster Amazon Aurora ed Hermes gestiti da Amazon Relational Database Service (Amazon RDS). La regola è NON_COMPLIANT se Multi-AZ non è configurato per un'istanza Amazon RDS.

Identificatore: RDS_CLUSTER_MULTI_AZ_ENABLED

Tipi di risorse: AWS::RDS::DBCluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-db-security-group-not-allowed

Verifica se esistono gruppi di sicurezza database di Amazon Relational Database Service (Amazon RDS) diversi dal gruppo di sicurezza database predefinito. La regola è NON_COMPLIANT se esistono gruppi di sicurezza database diversi dal gruppo di sicurezza database predefinito.

Identificatore: RDS_DB_SECURITY_GROUP_NOT_ALLOWED

Tipi di risorse: AWS: :RDS: :DB SecurityGroup

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile soltanto nelle regioni Europa (Irlanda), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Tokyo), Stati Uniti occidentali (Oregon), Stati Uniti occidentali (California settentrionale), Asia Pacifico (Singapore), Asia Pacifico (Sydney)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-enhanced-monitoring-enabled

Verifica se per le istanze Amazon RDS è abilitato il monitoraggio avanzato. Questa regola è NON_COMPLIANT se "`monitoringInterval`" è "0" nell'elemento di configurazione dell'istanza RDS o se "`monitoringInterval`" non corrisponde al valore del parametro della regola.

Identificatore: RDS_ENHANCED_MONITORING_ENABLED

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

monitoringInterval (opzionale), Tipo: int

> Un valore intero in secondi tra i punti quando vengono raccolte metriche di monitoraggio avanzate per l'istanza del database. I valori validi sono 1, 5, 10, 15, 30 e 60.

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
```

```
    "Engine": String*
}
...
```

* Per ulteriori informazioni sui valori validi per questi input, vedere MonitoringIntervaland Engine nella Guida per l'utente. AWS CloudFormation

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-instance-default-admin-check

Verifica se il nome utente amministratore di un database Amazon Relational Database Service (Amazon RDS) è diverso rispetto al valore predefinito. Questa regola viene eseguita solo su istanze database RDS. La regola è NON_COMPLIANT se il nome utente amministratore è impostato sul valore predefinito.

Identificatore: RDS_INSTANCE_DEFAULT_ADMIN_CHECK

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

valido AdminUserNames (facoltativo), Tipo: CSV

> Elenco separato da virgole dei nomi utente amministratore che le istanze Amazon RDS possono utilizzare (non è possibile includere "postgres" o "admin" come nomi utente validi poiché si tratta di valori predefiniti).

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-instance-deletion-protection-enabled

Verifica se la protezione dall'eliminazione è abilitata per un'istanza Amazon Relational Database Service (Amazon RDS). La regola è NON_COMPLIANT se la protezione dall'eliminazione non è abilitata per un'istanza Amazon RDS; ad esempio se deletionProtection è impostato su false.

> **Warning**
>
> Alcune istanze database RDS all'interno di un cluster (Aurora/DocumentDB) vengono visualizzate come non conformi.

Identificatore: RDS_INSTANCE_DELETION_PROTECTION_ENABLED

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

databaseEngines (opzionale), Tipo: CSV

Elenco separato da virgole dei motori di database RDS da includere nella valutazione della regola. Ad esempio "mysql, postgres, mariadb".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

rds-instance-iam-authentication-enabled

Verifica se un'istanza di Amazon Relational Database Service (Amazon RDS) AWS ha l'autenticazione Identity and Access Management (IAM) abilitata. La regola è NON_COMPLIANT se l'autenticazione IAM non è abilitata per un'istanza Amazon RDS.

> **Note**
>
> Il motore di database deve essere uno tra "mysql", "postgres", "aurora", "aurora-mysql" o "aurora-postgresql". Lo stato dell'istanza database deve essere uno tra "available", "backing-up", "storage-optimization" o "storage-full".

Identificatore: RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-instance-public-access-check

Verifica se le istanze Amazon Relational Database Service (Amazon RDS) non sono pubblicamente accessibili. La regola è NON_COMPLIANT se il campo publiclyAccessible è true nell'elemento di configurazione dell'istanza.

Identifier (Identificatore): RDS_INSTANCE_PUBLIC_ACCESS_CHECK

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, vedi Valutazione delle risorse con AWS Config le regole. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-in-backup-plan

Verifica se i database Amazon Relational Database Service (Amazon RDS) sono presenti nei piani di AWS Backup. La regola è NON_COMPLIANT se i database Amazon RDS non sono inclusi in alcun piano di Backup. AWS

> **Note**
>
> La regola si applica solo alle istanze database Amazon Aurora. I cluster database non sono supportati.

Identificatore: RDS_IN_BACKUP_PLAN

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-last-backup-recovery-point-created

Verifica se è stato creato un punto di ripristino per Amazon Relational Database Service (Amazon RDS). La regola è NON_COMPLIANT se l'istanza Amazon RDS non dispone di un punto di ripristino corrispondente creato entro il periodo di tempo specificato.

Identificatore: RDS_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▬Tipo: stringa

Tag delle istanze Amazon RDS che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▬Tipo: stringa

ID dell'istanza Amazon RDS che la regola deve verificare.

ripristino PointAgeValue (opzionale), Tipo: int, Impostazione predefinita: 1

Valore numerico per la durata massima consentita. Non superiore a 744 per le ore e 31 per i giorni.

ripristino PointAgeUnit (opzionale), ▬Tipo: stringa, Impostazione predefinita: giorni

Unità di tempo per la durata massima consentita. Valori accettati: "ore", "giorni".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-logging-enabled

Verifica se i rispettivi log di Amazon Relational Database Service (Amazon RDS) sono abilitati. La regola è NON_COMPLIANT se non è abilitato alcun tipo di log.

> **Note**
>
> Le istanze database che non sono nello stato "available", "backing-up", "storage-optimization" o "storage-full" vengono valutate come `NOT_APPLICABLE`.

Identificatore: RDS_LOGGING_ENABLED

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

additionalLogs (opzionale), Tipo: StringMap

Elenco separato da virgole dei nomi dei motori e dei tipi di log. Ad esempio "additionalLogs": "oracle: general, slowquery ; aurora: alert, slowquery"

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-meets-restore-time-target

Verifica se il tempo di ripristino delle istanze Amazon Relational Database Service (Amazon RDS) soddisfa la durata specificata. La regola è NON_COMPLIANT se LatestRestoreExecutionTimeMinutes un'istanza Amazon RDS dura più di minuti. maxRestoreTime

Identificatore: RDS_MEETS_RESTORE_TIME_TARGET

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Periodico

Regione AWS: AWS Tutte le regioni supportate

Parametri:

max RestoreTime, Tipo: int

Valore numerico per il runtime massimo di ripristino consentito.

resourceTags (opzionale), ▬Tipo: stringa

Tag delle istanze Amazon RDS che la regola deve verificare, in formato JSON .

resourceId (opzionale), ▬Tipo: stringa

ID dell'istanza Amazon RDS che la regola deve verificare.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-multi-az-support

Verifica se per le istanze database RDS è abilitata l'alta disponibilità.

In un'implementazione Multi-AZ, Amazon RDS effettua automaticamente il provisioning e mantiene una replica standby sincrona in un'altra zona di disponibilità. Per ulteriori informazioni, consulta Configurazione e gestione di un'implementazione multi-AZ nella Guida per l'utente di Amazon RDS.

> **Note**
>
> Questa regola non valuta le istanze database Amazon Aurora, Amazon DocumentDB e Amazon Neptune.

Identificatore: RDS_MULTI_AZ_SUPPORT

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
    "MultiAZ": BOOLEAN*,
    "Engine": String*
}
...
```

* Per ulteriori informazioni sui valori validi per questi ingressi, vedere MultiaZ and Engine nella Guida per l'utente. AWS CloudFormation

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-resources-protected-by-backup-plan

Verifica se le istanze Amazon Relational Database Service (Amazon RDS) sono protette da un piano di backup. La regola è NON_COMPLIANT se l'istanza database Amazon RDS non è coperta da un piano di backup.

Identificatore: RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▪Tipo: stringa

Tag per le istanze Amazon RDS che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▪Tipo: stringa

ID dell'istanza Amazon RDS che la regola deve verificare.

crossRegionList (Facoltativo), ▪Tipo: stringa

Elenco separato da virgole delle regioni di destinazione della copia di backup tra regioni da conservare

crossAccountList (Opzionale), ▪Tipo: stringa

Elenco separato da virgole degli account di destinazione della copia di backup tra account da conservare

maxRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione massimo in giorni per Vault Lock di Backup

minRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione minimo in giorni per Vault Lock di Backup

backup VaultLockCheck (opzionale), ▪Tipo: stringa

Valori accettati: "True" o "False". Immetti "True" per fare in modo che la regola verifichi se per la risorsa viene eseguito il backup in un vault bloccato

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-snapshots-public-prohibited

Verifica se gli snapshot Amazon Relational Database Service (Amazon RDS) sono pubblici. La regola è NON_COMPLIANT se gli snapshot Amazon RDS esistenti o nuovi sono pubblici..

> **Note**
>
> Possono essere necessarie fino a 12 ore affinché i risultati di conformità vengano acquisiti.

Identificatore: RDS_SNAPSHOTS_PUBLIC_PROHIBITED

Tipi di risorse: AWS: :RDS: :DBSnapshot, AWS: :RDS: :DB ClusterSnapshot

Tipo di trigger: Modifiche alla configurazione

Regione AWS AWS : Tutte le regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-snapshot-encrypted

Verifica se gli snapshot di database Amazon Relational Database Service (Amazon RDS) sono crittografati. La regola è NON_COMPLIANT, se gli snapshot di database Amazon RDS non sono crittografati.

Identificatore: RDS_SNAPSHOT_ENCRYPTED

Tipi di risorse: AWS: :RDS: :DBSnapshot, AWS: :RDS: :DB ClusterSnapshot

Tipo di trigger: Modifiche alla configurazione

Regione AWS AWS : Tutte le regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

rds-storage-encrypted

Verifica se la crittografia di archiviazione è abilitata per le istanze database Amazon Relational Database Service (Amazon RDS). La regola è NON_COMPLIANT se la crittografia di archiviazione non è abilitata.

Identificatore: RDS_STORAGE_ENCRYPTED

Tipi di risorse: AWS::RDS::DBInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsKeyId (Facoltativo), ▬Tipo: stringa

ID o nome della risorsa Amazon (ARN) della chiave KMS usato per crittografare l'archiviazione.

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
   "StorageEncrypted": BOOLEAN
}
```

```
...
```

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

redshift-audit-logging-enabled

Verifica se i cluster Amazon Redshift effettuano la registrazione di log di audit su un bucket specifico. La regola è NON_COMPLIANT se la registrazione di log di audit non è abilitata per un cluster Redshift o se viene fornito il parametro "`bucketNames`", ma la destinazione della registrazione di log di audit non corrisponde.

Identificatore: REDSHIFT_AUDIT_LOGGING_ENABLED

Tipi di risorse: AWS::Redshift::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

bucketNames (opzionale), Tipo: CSV

Elenco separato da virgole dei nomi di bucket Amazon S3 per l'archiviazione dei log di audit.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

redshift-backup-enabled

Verifica se gli snapshot automatici Amazon Redshift sono abilitati per i cluster. La regola è NON_COMPLIANT se il valore per `automatedSnapshotRetentionPeriod` è maggiore di `MaxRetentionPeriod` o minore di `MinRetentionPeriod` o se è pari a 0.

Identificatore: REDSHIFT_BACKUP_ENABLED

Tipi di risorse: AWS::Redshift::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

MinRetentionPeriod (Facoltativo), Tipo: int

Valore minimo per il periodo di conservazione. Il valore minimo è 1.

MaxRetentionPeriod (Opzionale), Tipo: int

Valore massimo per il periodo di conservazione. Il valore massimo è 35.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

redshift-cluster-configuration-check

Verifica se i cluster Amazon Redshift hanno le impostazioni specificate. La regola è NON_COMPLIANT se il cluster Amazon Redshift non è crittografato, se è crittografato con un'altra chiave o se la registrazione di log di audit non è abilitata per il cluster.

Identificatore: REDSHIFT_CLUSTER_CONFIGURATION_CHECK

Tipi di risorse: AWS::Redshift::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

cluster DbEncrypted, Tipo: booleano, Impostazione predefinita: true

La crittografia del database è abilitata.

loggingEnabled, Tipo: booleano, Impostazione predefinita: true

La registrazione di log di audit è abilitata.

nodeTypes (opzionale), Tipo: CSV, Impostazione predefinita: dc1.large

Specifica il tipo di nodo.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

redshift-cluster-kms-enabled

Verifica se i cluster Amazon Redshift utilizzano una chiave specificata AWS Key Management Service (AWS KMS) per la crittografia. La regola è COMPLIANT se la crittografia è abilitata e il cluster è crittografato con la chiave fornita nel parametro `kmsKeyArn`. La regola è NON_COMPLIANT se il cluster non è crittografato o se è crittografato con un'altra chiave.

Identificatore: REDSHIFT_CLUSTER_KMS_ENABLED

Tipi di risorse: AWS::Redshift::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsKeyArns (Facoltativo), Tipo: CSV

Elenco separato da virgole delle chiavi AWS KMS Amazon Resource Names (ARN) utilizzate nei cluster Amazon Redshift per la crittografia.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

redshift-cluster-maintenancesettings-check

Verifica se sono state specificate delle impostazioni di manutenzione per i cluster Amazon Redshift. La regola è NON_COMPLIANT se gli aggiornamenti automatici alla versione principale sono disabilitati.

Identificatore: REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

Tipi di risorse: AWS::Redshift::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

consentire VersionUpgrade, Tipo: booleano, Impostazione predefinita: true

L'opzione Consenti aggiornamento della versione è abilitata.

preferredMaintenanceWindow (Facoltativo), ▬Tipo: stringa

Finestra di manutenzione pianificata per i cluster, ad esempio lun 9.30-lun 10.00.

automatizzato SnapshotRetentionPeriod (opzionale), Tipo: int, Impostazione predefinita: 1

Numero di giorni per cui conservare gli snapshot automatizzati.

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
...
```

* Per ulteriori informazioni sui valori validi per questi input AutomatedSnapshotRetentionPeriod, vedere PreferredMaintenanceWindow e AllowVersion Upgrade nella Guida per l'utente. AWS CloudFormation

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

redshift-cluster-public-access-check

Verifica se i cluster Amazon Redshift non sono accessibili pubblicamente. La regola è NON_COMPLIANT se il campo publiclyAccessible è True nell'elemento di configurazione del cluster.

Identificatore: REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

Tipi di risorse: AWS::Redshift::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

redshift-default-admin-check

Verifica se il nome utente amministratore di un cluster Amazon Redshift è diverso rispetto al valore predefinito. La regola è NON_COMPLIANT se il nome utente amministratore di un cluster Redshift è impostato su "awsuser" o se il nome utente non corrisponde a quanto elencato nel parametro.

Identificatore: REDSHIFT_DEFAULT_ADMIN_CHECK

Tipi di risorse: AWS::Redshift::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

valido AdminUserNames (opzionale), Tipo: CSV

> Elenco separato da virgole dei nomi utente amministratore che i cluster Redshift devono utilizzare. Nota: "awsuser" è l'impostazione predefinita e non è accettato.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

redshift-default-db-name-check

Verifica se il nome di database di un cluster Redshift è diverso rispetto al valore predefinito. La regola è NON_COMPLIANT se il nome di database di un cluster Redshift è impostato su "dev" o se viene fornito il parametro opzionale e il nome di database non corrisponde.

Identificatore: REDSHIFT_DEFAULT_DB_NAME_CHECK

Tipi di risorse: AWS::Redshift::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

validDatabaseNames (Facoltativo), Tipo: CSV

Elenco separato da virgole dei nomi di database dei cluster Redshift.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

redshift-enhanced-vpc-routing-enabled

Verifica se il cluster Amazon Redshift è abilitato per «Enhanced»VpcRouting. La regola è NON_COMPLIANT se «enhancedVpcRouting» non è abilitato o se la configurazione è disabilitata. enhancedVpcRouting il campo è 'falso'.

Identificatore: REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED

Tipi di risorse: AWS::Redshift::Cluster

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

redshift-require-tls-ssl

Verifica se i cluster Amazon Redshift richiedono la crittografia TLS/SSL per connettersi ai client SQL. La regola è NON_COMPLIANT se il parametro require_SSL di un qualsiasi cluster Amazon Redshift non è impostato su true.

Identificatore: REDSHIFT_REQUIRE_TLS_SSL

Tipi di risorse: AWS::Redshift::Cluster, AWS::Redshift::ClusterParameter Gruppo

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

redshift - accesso alle porte senza restrizioni

Verifica se i gruppi di sicurezza associati a un cluster Amazon Redshift dispongono di regole in entrata che consentono il traffico in entrata senza restrizioni. La regola è NON_COMPLIANT se esistono regole in entrata che consentono il traffico in entrata senza restrizioni verso la porta del cluster Redshift.

Identificatore: REDSHIFT_UNRESTRICTED_PORT_ACCESS

Tipi di risorse: AWS::Redshift::Cluster

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

required-tags

Verifica se per le risorse sono presenti i tag specificati. Ad esempio, puoi verificare se le istanze Amazon EC2 hanno il tag `CostCenter` e allo stesso tempo verificare se a tutte le istanze RDS è applicato un set di tag Keys. Separa più valori con virgole. Puoi verificare fino a 6 tag alla volta.

Il documento AWS di AWS Systems Manager automazione gestito `AWS-SetRequiredTags` non funziona come rimedio con questa regola. Sarà necessario la propria documentazione di automazione personalizzata di Systems Manager per la riparazione.

Contesto: AWS consente di assegnare metadati alle AWS risorse sotto forma di tag. Ogni tag è un'etichetta composta da una chiave e da un valore opzionale per archiviare le informazioni sulla risorsa o i dati mantenuti su quest'ultima. Per ulteriori informazioni, consulta Sviluppo della strategia di assegnazione di tag.

Puoi utilizzare questa regola per trovare le risorse nell'account che non sono state avviate con le configurazioni desiderate, specificando quali risorse devono avere tag e il valore previsto per ogni tag. Puoi inoltre eseguire azioni di riparazione per correggere gli errori di assegnazione di tag. Tuttavia, questa regola non impedisce di creare risorse con tag errati.

Identificatore: REQUIRED_TAGS

Tipi di risorse: AWS::ACM::Certificate, AWS::AutoScaling:: AutoScaling Group, AWS::CloudFormation::Stack, AWS::CodeBuild: :Project, AWS::DynamoDB::Table, AWS::EC2::CustomerGateway, AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkAcl, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable, AWS::EC2::SecurityGroup,, AWS::EC2::Subnet, AWS::EC2::Volume, AWS::EC2::VPC, AWS::EC2::VPNConnection, AWS::EC2::VPNGateway, AWS::ElasticLoad Bilanciamento:: LoadBalancer AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::RDS::DBInstance, AWS::RDS::DBSecurityGroup, AWS::RDS::DBSnapshot, AWS::RDS::DBSubnetGroup, AWS::RDS::EventSubscription, AWS::Redshift::Cluster, AWS::Redshift::ClusterParameter Group, AWS::Redshift::ClusterSecurity Group, AWS::Redshift::ClusterSnapshot AWS::Redshift::ClusterSubnet AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

tag1Key, ▬Tipo: stringa, Impostazione predefinita: CostCenter

Chiave del tag richiesto.

tag1Value (opzionale), Tipo: CSV

Valore facoltativo del tag richiesto. Separa più valori con virgole.

tag2key (opzionale), ▪Tipo: stringa

Chiave di un secondo tag obbligatorio.

tag2Value (opzionale), Tipo: CSV

Valore opzionale del secondo tag obbligatorio. Separa più valori con virgole.

tag3Key (opzionale), ▪Tipo: stringa

Chiave del terzo tag obbligatorio.

tag3Value (opzionale), Tipo: CSV

Valore opzionale del terzo tag obbligatorio. Separa più valori con virgole.

tag4Key (opzionale), ▪Tipo: stringa

Chiave del quarto tag obbligatorio.

tag4Value (opzionale), Tipo: CSV

Valore opzionale del quarto tag obbligatorio. Separa più valori con virgole.

tag5Key (opzionale), ▪Tipo: stringa

Chiave del quinto tag obbligatorio.

tag5Value (opzionale), Tipo: CSV

Valore opzionale del quinto tag obbligatorio. Separa più valori con virgole.

tag6Key (opzionale), ▪Tipo: stringa

Chiave del sesto tag obbligatorio.

tag6Value (opzionale), Tipo: CSV

Valore opzionale del sesto tag obbligatorio. Separa più valori con virgole.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere Creazione di regole gestite di AWS Config con modelli AWS CloudFormation.

restricted-common-ports

> **Important**
>
> Per questa regola, l'identificatore (RESTRICTED_INCOMING_TRAFFIC) e il nome della regola (restricted-common-ports) sono diversi.

Verifica se i gruppi di sicurezza in uso non consentono il traffico TCP (Transmission Control Protocol) illimitato in entrata sulle porte specificate. La regola è COMPLIANT se:

- L'accesso alle porte è bloccato a tutto il traffico TCP.
- L'accesso alle porte è aperto al traffico TCP tramite regole in entrata, in cui l'origine è un singolo indirizzo IPv4 o un intervallo di indirizzi IPv4 in notazione CIDR che non copre tutti gli indirizzi IPv4 ("0.0.0.0/0").
- L'accesso alle porte è aperto al traffico TCP tramite regole in entrata, in cui l'origine è un singolo indirizzo IPv6 o un intervallo di indirizzi IPv6 in notazione CIDR che non copre tutti gli indirizzi IPv6 ("::/0)").

La regola è NON_COMPLIANT se gli indirizzi IP per le connessioni TCP in entrata non sono limitati alle porte specificate.

Identificatore: RESTRICTED_INCOMING_TRAFFIC

Tipi di risorse: AWS::EC2::SecurityGroup

Tipo di trigger: Modifiche alla configurazione e periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

blockedPort1 (opzionale), Tipo: int, Impostazione predefinita: 20

Numero di porta TCP bloccata. L'impostazione predefinita di 20 corrisponde al trasferimento dati FTP (File Transfer Protocol).

blockedPort2 (opzionale), Tipo: int, Impostazione predefinita: 21

Numero di porta TCP bloccata. L'impostazione predefinita di 21 corrisponde al controllo dei comandi FTP (File Transfer Protocol).

blockedPort3 (opzionale), Tipo: int, Impostazione predefinita: 3389

Numero di porta TCP bloccata. L'impostazione predefinita di 3389 corrisponde al protocollo RDP (Remote Desktop Protocol).

blockedPort4 (opzionale), Tipo: int, Impostazione predefinita: 3306

Numero di porta TCP bloccata. L'impostazione predefinita di 3306 corrisponde al protocollo MySQL.

blockedPort5 (opzionale), Tipo: int, Impostazione predefinita: 4333

Numero di porta TCP bloccata. L'impostazione predefinita di 4333 corrisponde al protocollo MySQL.

blockedPorts (opzionale), Tipo: CSV

Elenco separato da virgole dei numeri di porta TCP bloccati. Ad esempio 20, 21, 3306, 3389 e 4333.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

root-account-hardware-mfa-enabled

Verifica se il tuo AWS account è abilitato all'uso del dispositivo hardware di autenticazione a più fattori (MFA) per accedere con le credenziali root. La regola è NON_COMPLIANT se ai dispositivi MFA virtuali è consentito l'accesso con le credenziali root.

> **Note**
>
> Regole gestite e tipi di risorse IAM globali
> I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.
> Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le

regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.
Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.

Identifier (Identificatore): ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

Tipo di trigger: Periodico

Regione AWS: tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

root-account-mfa-enabled

Verifica se l'utente root del tuo AWS account richiede l'autenticazione a più fattori per l'accesso alla console. La regola è NON_COMPLIANT se l'utente dell'account root AWS Identity and Access Management (IAM) non ha l'autenticazione a più fattori (MFA) abilitata.

> **Note**
>
> Regole gestite e tipi di risorse IAM globali
> I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`AWS::IAM::Role, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.
> Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le

regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.
Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.

Identificatore: ROOT_ACCOUNT_MFA_ENABLED

Tipo di trigger: Periodico

Regione AWS: tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

route53-query-logging-enabled

Verifica se la registrazione di log delle query DNS è abilitata per le zone ospitate pubbliche di Amazon Route 53. La regola è NON_COMPLIANT se la registrazione di log delle query DNS non è abilitata per le zone ospitate pubbliche di Amazon Route 53.

Identificatore: ROUTE53_QUERY_LOGGING_ENABLED

Tipi di risorse: AWS::Route53::HostedZone

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-access-point-in-vpc-only

Verifica se un punto di accesso Amazon S3 non consente l'accesso da Internet (è NetworkOrigin VPC). La regola è NON_COMPLIANT se è Internet. NetworkOrigin

Identificatore: S3_ACCESS_POINT_IN_VPC_ONLY

Tipi di risorse: AWS::S3::AccessPoint

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-access-point-public-access-blocks

Verifica se le impostazioni di blocco dell'accesso pubblico sono abilitate per i punti di accesso Amazon S3. La regola è NON_COMPLIANT se le impostazioni di blocco dell'accesso pubblico non sono abilitate per i punti di accesso S3.

Identificatore: S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

Tipi di risorse: AWS::S3::AccessPoint

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

excludedAccessPoints (Facoltativo), Tipo: CSV

Elenco separato da virgole dei nomi dei punti di accesso Amazon S3 pubblici consentiti.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-account-level-public-access-blocks

Verifica se le impostazioni di blocco dell'accesso pubblico richieste sono configurate a livello di account. La regola è solo NON_COMPLIANT quando i campi impostati di seguito non corrispondono ai campi corrispondenti nell'elemento di configurazione.

> **Note**
>
> Se utilizzi questa regola, assicurati che il blocco dell'accesso pubblico di S3 sia abilitato. La regola viene attivata dalle modifiche, quindi non verrà richiamata a meno che il blocco dell'accesso pubblico di S3 non sia abilitato. Se il blocco dell'accesso pubblico di S3 non è abilitato, la regola restituisce INSUFFICIENT_DATA. Ciò significa che potrebbero esserci ancora alcuni bucket pubblici. Per ulteriori informazioni sulla configurazione del blocco dell'accesso pubblico di S3, consulta Blocco dell'accesso pubblico allo storage Amazon S3.

Identificatore: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

Tipi di risorse: AWS::S3::AccountPublic AccessBlock

Tipo di trigger: modifiche alla configurazione (lo stato attuale non viene verificato, la valutazione viene avviata solo quando le modifiche generano nuovi eventi)

> **Note**
>
> Questa regola viene attivata solo dalle modifiche alla configurazione per la regione specifica in cui si trova l'endpoint S3. In tutte le altre regioni, la regola viene verificata periodicamente. Se è stata apportata una modifica in un'altra regione, potrebbe verificarsi un ritardo prima che la regola restituisca NON_COMPLIANT.

Regione AWS: Tutte le AWS regioni supportate

Parametri:

IgnorePublicAcls (Facoltativo), ▪Tipo: stringa, Impostazione predefinita: True

IgnorePublicAcls è applicato o meno, impostazione predefinita True

BlockPublicPolicy (Facoltativo), ▪Tipo: stringa, Impostazione predefinita: True

BlockPublicPolicy è applicato o meno, impostazione predefinita True

BlockPublicAcls (Facoltativo), ▪Tipo: stringa, Impostazione predefinita: True

BlockPublicAcls è applicato o meno, impostazione predefinita True

RestrictPublicBuckets (Facoltativo), ▪Tipo: stringa, Impostazione predefinita: True

RestrictPublicBuckets è applicato o meno, impostazione predefinita True

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

s3-account-level-public-access-blocks-periodic

Verifica se le impostazioni di blocco dell'accesso pubblico richieste sono configurate a livello di account. La regola è NON_COMPLIANT se l'elemento di configurazione non corrisponde a una o più impostazioni dei parametri (o predefinite).

Identificatore: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

Tipi di risorse: AWS::::Account

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

IgnorePublicAcls (Facoltativo), ▪Tipo: stringa

IgnorePublicAcls è applicato o meno, impostazione predefinita True

BlockPublicPolicy (Facoltativo), ▪Tipo: stringa

BlockPublicPolicy è applicato o meno, impostazione predefinita True

BlockPublicAcls (Facoltativo), ▪Tipo: stringa

BlockPublicAcls è applicato o meno, impostazione predefinita True

RestrictPublicBuckets (Facoltativo), ▪Tipo: stringa

RestrictPublicBuckets è applicato o meno, impostazione predefinita True

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-acl-prohibited

Verifica se i bucket Amazon Simple Storage Service (Amazon S3) consentono le autorizzazioni utente tramite le liste di controllo degli accessi (ACL). La regola è NON_COMPLIANT se le ACL sono configurate per l'accesso degli utenti nei bucket Amazon S3.

Identificatore: S3_BUCKET_ACL_PROIBITED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-blacklisted-actions-prohibited

Verifica se una policy sui bucket di Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) non consente azioni bloccate a livello di bucket e a livello di oggetto sulle

risorse del bucket per i principali di altri account. AWS Ad esempio, la regola verifica che la policy del bucket di Amazon S3 non consenta a un altro AWS account di eseguire `s3:GetBucket*` azioni e `s3:DeleteObject` su alcun oggetto nel bucket. La regola è NON_COMPLIANT se la policy del bucket Amazon S3 consente azioni inserite in blacklist.

> **Note**
>
> La regola verifica solo le entità nella proprietà Principal e non tiene conto dei condizionali previsti dalla proprietà Condition della policy

Identificatore: S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

nella lista nera ActionPattern, Tipo: CSV

Elenco separato da virgole di modelli di azione nella lista nera, ad esempio s3: * e s3:. GetBucket DeleteObject

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

abilitato per la replica tra più regioni con bucket s3

Verifica se hai abilitato la replica tra regioni S3 per i tuoi bucket Amazon S3. La regola è NON_COMPLIANT se non ci sono regole di replica abilitate per la replica tra regioni.

Identificatore: S3_BUCKET_CROSS_REGION_REPLICATION_ENABLED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-default-lock-enabled

Verifica se il blocco è abilitato per impostazione predefinita per il bucket S3. La regola è NON_COMPLIANT se il blocco non è abilitato.

Identificatore: S3_BUCKET_DEFAULT_LOCK_ENABLED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Modalità (Facoltativo), ▪Tipo: stringa

mode: (opzionale): un parametro di modalità con valori validi di GOVERNANCE o COMPLIANCE.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-level-public-access-prohibited

Verifica se i bucket S3 sono accessibili pubblicamente. La regola è NON_COMPLIANT se un bucket S3 non è elencato nel parametro `excludedPublicBuckets` e se le impostazioni a livello di bucket sono pubbliche.

Identificatore: S3_BUCKET_LEVEL_PUBLIC_ACCESS_FORBIDDEN

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

excludedPublicBuckets (Facoltativo), Tipo: CSV

Elenco separato da virgole dei nomi dei bucket Amazon S3 pubblici consentiti.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-logging-enabled

Verifica se la registrazione di log è abilitata per i bucket S3. La regola è NON_COMPLIANT se il campo logging non è abilitato.

Identificatore: S3_BUCKET_LOGGING_ENABLED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

targetBucket (opzionale), ▪Tipo: stringa

Il bucket S3 di destinazione per l'archiviazione dei log di accesso al server.

targetPrefix (opzionale), ▪Tipo: stringa

Prefisso del bucket S3 per l'archiviazione dei log di accesso al server.

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
   "BucketName": "my-bucket",
   "LoggingConfiguration": {
         "DestinationBucketName": "my-log-bucket",
         "LogFilePrefix":"my-log"
   }
}
...
```

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-mfa-delete-enabled

Verifica se l'eliminazione MFA è abilitata nella configurazione del controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3). La regola è NON_COMPLIANT se l'eliminazione MFA non è abilitata.

Identificatore: S3_BUCKET_MFA_DELETE_ENABLED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-policy-grantee-check

Verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dai VPC che fornisci. La regola è COMPLIANT se una policy del bucket non è disponibile.

Ad esempio, se il parametro di input per la regola è l'elenco di due principali: `111122223333` e `444455556666` e la policy del bucket specifica che solo `111122223333` può accedere al bucket, allora la regola è COMPLIANT. Con gli stessi parametri di input: se la policy dei bucket specifica che `111122223333` e `444455556666` possono accedere al bucket, è anche conforme. Tuttavia, se la policy dei bucket specifica che `999900009999` può accedere al bucket, la regola è NON-COMPLIANT.

> **Note**
>
> Se una policy del bucket contiene più di un'istruzione, ogni istruzione in tale policy viene valutata in base a questa regola.

Identifier (Identificatore): S3_BUCKET_POLICY_GRANTEE_CHECK

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

awsPrincipals (opzionale), Tipo: CSV

Elenco separato da virgole di principali come IAM User ARN, IAM Role ARN e AWS account, ad esempio 'arn:aws:iam: :111122223333:user/Alice, arn:aws:iam: :444455556666:role/BOB, 123456789012'.

servicePrincipals (opzionale), Tipo: CSV

Elenco separato da virgole dei principali del servizio, ad esempio "cloudtrail.amazonaws.com, lambda.amazonaws.com".

federatedUsers (opzionale), Tipo: CSV

Elenco separato da virgole dei provider di identità per la federazione delle identità Web, ad esempio Amazon Cognito e i provider di identità SAML. Ad esempio "cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider".

ipAddresses (opzionale), Tipo: CSV

Elenco separato da virgole degli indirizzi IP in formato CIDR, ad esempio "10.0.0.1, 192.168.1.0/24, 2001:db8::/32".

vpcIds (opzionale), Tipo: CSV

Elenco separato da virgole degli ID Amazon Virtual Private Cloud (Amazon VPC), ad esempio "vpc-1234abc0, vpc-ab1234c0".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

s3-bucket-policy-not-more-permissive

Verifica se le policy del bucket Amazon Simple Storage Service non consentono altre autorizzazioni tra account oltre alla policy di controllo per il bucket Amazon S3 specificata.

> **Note**
>
> Se fornisci un valore di parametro non valido, verrà visualizzato il seguente messaggio di errore: Il valore del parametro controlPolicy deve essere una policy del bucket Amazon S3.

Identificatore: S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

controlPolicy, ▪Tipo: stringa

La policy dei bucket Amazon S3 che definisce un limite superiore per le autorizzazioni dei bucket S3. La lunghezza massima della policy è 1024 caratteri.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-public-read-prohibited

Verifica se i bucket Amazon S3 non permettono l'accesso pubblico in lettura. La regola verifica le impostazioni di blocco dell'accesso pubblico, la policy del bucket e la lista di controllo accessi (ACL) del bucket.

La regola è conforme quando sono vere entrambe le condizioni seguenti:

- L'impostazione di blocco dell'accesso pubblico limita le policy pubbliche o la policy del bucket non consente l'accesso pubblico in lettura.
- L'impostazione di blocca dell'accesso pubblico limita gli ACL pubblici o l'ACL del bucket non consente l'accesso pubblico in lettura.

La regola non è conforme:

- Se l'impostazione Blocca accesso pubblico non limita le politiche pubbliche, AWS Config valuta se la politica consente l'accesso pubblico in lettura. Se la policy consente l'accesso pubblico in lettura, la regola non è conforme.
- Se l'impostazione Block Public Access non limita gli ACL dei bucket pubblici, AWS Config valuta se l'ACL del bucket consente l'accesso pubblico in lettura. Se l'ACL del bucket consente l'accesso pubblico in lettura, la regola non è conforme.

Identificatore: S3_BUCKET_PUBLIC_READ_PROHIBITED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione e periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-public-write-prohibited

Verifica se i bucket Amazon S3 non permettono l'accesso pubblico in scrittura. La regola verifica le impostazioni di blocco dell'accesso pubblico, la policy del bucket e la lista di controllo accessi (ACL) del bucket.

La regola è conforme quando sono vere entrambe le condizioni seguenti:

- L'impostazione di blocco dell'accesso pubblico limita le policy pubbliche o la policy del bucket non consente l'accesso pubblico in scrittura.
- L'impostazione di blocca dell'accesso pubblico limita gli ACL pubblici o l'ACL del bucket non consente l'accesso pubblico in scrittura.

La regola non è conforme:

- Se l'impostazione Blocca accesso pubblico non limita le politiche pubbliche, AWS Config valuta se la politica consente l'accesso pubblico in scrittura. Se la policy consente l'accesso pubblico in scrittura, la regola non è conforme.
- Se l'impostazione Block Public Access non limita gli ACL dei bucket pubblici, AWS Config valuta se l'ACL del bucket consente l'accesso pubblico in scrittura. Se l'ACL del bucket consente l'accesso pubblico in scrittura, la regola non è conforme.

> **Note**
>
> Questa regola non valuta le modifiche al blocco dell'accesso pubblico a livello di account. Per verificare se le impostazioni richieste per il blocco dell'accesso pubblico sono configurate a

livello di account, consulta s3-account-level-public-access-blocks e s3-account-level-public-access-blocks-periodic.

Identificatore: S3_BUCKET_PUBLIC_WRITE_PROHIBITED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione e periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-replication-enabled

Verifica se i bucket S3 dispongono di regole di replica abilitate. La regola è NON_COMPLIANT se un bucket S3 non dispone di regole di replica o se il bucket dispone di una regola di replica non abilitata.

Identificatore: S3_BUCKET_REPLICATION_ENABLED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

ReplicationType (Facoltativo), ▬Tipo: stringa

Valori accettati: "CROSS-REGION" e "SAME-REGION". Immetti "CROSS-REGION" in modo che la regola verifichi se in tutti i bucket è abilitata solo la replica tra regioni. Immetti "SAME-REGION" in modo che la regola verifichi se in tutti i bucket è abilitata solo la replica nella stessa regione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-server-side-encryption-enabled

Verifica se la crittografia predefinita Amazon S3 è abilitata per il bucket Amazon S3 o se la policy del bucket Amazon S3 nega esplicitamente le richieste `put-object` senza la crittografia lato server con AES-256 o AWS Key Management Service. La regola è NON_COMPLIANT se il bucket Amazon S3 non è crittografato per impostazione predefinita.

Identificatore: S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-ssl-requests-only

Verifica se i bucket S3 dispongono di policy che richiedono l'utilizzo di SSL/TLS per le richieste. La regola è NON_COMPLIANT se un bucket S3 dispone di policy che consentono le richieste HTTP.

Identificatore: S3_BUCKET_SSL_REQUESTS_ONLY

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-bucket-versioning-enabled

Verifica se il controllo delle versioni è abilitato per i bucket S3. Facoltativamente, la regola verifica se l'eliminazione con MFA è abilitata per i bucket S3.

Identificatore: S3_BUCKET_VERSIONING_ENABLED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

è MfaDeleteEnabled (facoltativo), ▬Tipo: stringa

L'eliminazione con MFA è abilitata per i bucket S3.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-default-encryption-kms

Verifica se i bucket S3 sono crittografati con Key Management Service (KMS). AWS AWS La regola è NON_COMPLIANT se il bucket S3 non è crittografato con una chiave KMS. AWS

Identificatore: S3_DEFAULT_ENCRYPTION_KMS

AWS::S3::BucketTipi di risorse:, AWS::KMS::Key

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsKeyArns (Facoltativo), Tipo: CSV

Elenco separato da virgole di ARN di chiavi AWS KMS consentite per crittografare i bucket Amazon S3.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-event-notifications-enabled

Verifica se le notifiche sugli eventi Amazon S3 sono abilitate in un bucket S3. La regola è NON_COMPLIANT se le notifiche sugli eventi S3 non sono impostate su un bucket o se il tipo o la destinazione dell'evento non corrispondono ai parametri `eventTypes` e destinationArn.

Identificatore: S3_EVENT_NOTIFICATIONS_ENABLED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

destinationArn (opzionale), ▬Tipo: stringa

L'Amazon Resource Name (ARN) della destinazione per la notifica dell'evento (argomento Amazon SNS, AWS Lambda, Amazon SQS Queue).

eventTypes (opzionale), Tipo: CSV

Elenco separato da virgole dei tipi di eventi Amazon S3 preferiti

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-last-backup-recovery-point-created

Verifica se è stato creato un punto di ripristino per Amazon Simple Storage Service (Amazon S3). La regola è NON_COMPLIANT se il bucket Amazon S3 non dispone di un punto di ripristino corrispondente creato entro il periodo di tempo specificato.

Identificatore: S3_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▪Tipo: stringa

Tag del bucket Amazon S3 che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▪Tipo: stringa

Nome del bucket Amazon S3 che la regola deve verificare.

ripristino PointAgeValue (opzionale), Tipo: int, Impostazione predefinita: 1

Valore numerico per la durata massima consentita. Non superiore a 744 per le ore e 31 per i giorni.

ripristino PointAgeUnit (opzionale), ▪Tipo: stringa, Impostazione predefinita: giorni

Unità di tempo per la durata massima consentita. Valori accettati: "ore", "giorni".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

s3-lifecycle-policy-check

Verifica se una regola del ciclo di vita è configurata per un bucket Amazon Simple Storage Service (Amazon S3). La regola è NON_COMPLIANT se non ci sono regole di configurazione del ciclo di vita attive o se la configurazione non corrisponde ai valori dei parametri.

Identificatore: S3_LIFECYCLE_POLICY_CHECK

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

targetTransitionDays (Facoltativo), Tipo: int

Numero di giorni dopo la creazione di un oggetto in cui quest'ultimo viene trasferito a un classe di archiviazione specificata (ad esempio 30 giorni).

targetExpirationDays (Opzionale), Tipo: int

Numero di giorni dopo la creazione di un oggetto in cui quest'ultimo viene eliminato (ad esempio 395 giorni).

obiettivo TransitionStorageClass (opzionale), ▬Tipo: stringa

Tipo di classe di archiviazione di destinazione, ad esempio Accesso Infrequente Amazon S3 Standard (AI S3 Standard). Per ulteriori informazioni, consulta https: //docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html.

targetPrefix (opzionale), ▬Tipo: stringa

Prefisso dell'oggetto Amazon S3 per identificare uno o più oggetti.

bucketNames (opzionale), Tipo: CSV

Elenco separato da virgole dei nomi di bucket Amazon S3 con policy del ciclo di vita abilitate.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-meets-restore-time-target

Controlla se il tempo di ripristino dei bucket Amazon Simple Storage Service (Amazon S3) soddisfa la durata specificata. La regola è NON_COMPLIANT se un bucket LatestRestoreExecutionTimeMinutes Amazon S3 dura più di minuti. maxRestoreTime

Identificatore: S3_MEETS_RESTORE_TIME_TARGET

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

max RestoreTime, Tipo: int

Valore numerico per il runtime massimo di ripristino consentito.

resourceTags (opzionale), ▪Tipo: stringa

Tag del bucket Amazon S3 che la regola deve verificare, in formato JSON .

resourceId (opzionale), ▪Tipo: stringa

Nome del bucket Amazon S3 che la regola deve verificare.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

s3-resources-protected-by-backup-plan

Verifica se i bucket Amazon Simple Storage Service (Amazon S3) sono protetti da un piano di backup. La regola è NON_COMPLIANT se il bucket Amazon S3 non è coperto da un piano di backup.

Identificatore: S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▪Tipo: stringa

Tag dei bucket Amazon S3 che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), ▪Tipo: stringa

Nome del bucket Amazon S3 che la regola deve verificare.

crossRegionList (Facoltativo), ▪Tipo: stringa

Elenco separato da virgole delle regioni di destinazione della copia di backup tra regioni da conservare

crossAccountList (Opzionale), ▪Tipo: stringa

Elenco separato da virgole degli account di destinazione della copia di backup tra account da conservare

maxRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione massimo in giorni per Vault Lock di Backup

minRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione minimo in giorni per Vault Lock di Backup

backup VaultLockCheck (opzionale), ▪Tipo: stringa

Valori accettati: "True" o "False". Immetti "True" per fare in modo che la regola verifichi se per la risorsa viene eseguito il backup in un vault bloccato

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

s3-version-lifecycle-policy-check

Verifica se per i bucket abilitati per la versione di Amazon Simple Storage Service (Amazon S3) è configurata una policy del ciclo di vita. La regola è NON_COMPLIANT se la policy del ciclo di vita di Amazon S3 non è abilitata.

Identificatore: S3_VERSION_LIFECYCLE_POLICY_CHECK

Tipi di risorse: AWS::S3::Bucket

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

bucketNames (opzionale), Tipo: CSV

Elenco separato da virgole dei nomi di bucket Amazon S3 con policy del ciclo di vita abilitate.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

sagemaker-endpoint-configuration-kms-key-configured

Verifica se AWS la chiave Key Management Service (AWS KMS) è configurata per una configurazione di SageMaker endpoint Amazon. La regola è NON_COMPLIANT se non è specificato 'KmsKeyId' per la configurazione degli endpoint Amazon. SageMaker

Identificatore: SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

Tipi di risorse: AWS::SageMaker::EndpointConfig

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsKeyArns (Facoltativo), ▪Tipo: stringa

Elenco separato da virgole di ARN di chiavi AWS KMS specifiche consentite per una configurazione di endpoint Amazon. SageMaker

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

sagemaker-endpoint-config-prod-instance-count

Verifica se le configurazioni SageMaker degli endpoint di Amazon hanno varianti di produzione `InitialInstanceCount` impostate su un valore maggiore di 1. La regola è NON_COMPLIANT se le varianti di produzione `Count` sono uguali a 1. InitialInstance

Identificatore: SAGEMAKER_ENDPOINT_CONFIG_PROD_INSTANCE_COUNT

Tipi di risorse: AWS::SageMaker::EndpointConfig

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

sagemaker-notebook-instance-inside-vpc

Verifica se un'istanza di SageMaker notebook Amazon viene avviata all'interno di un VPC o all'interno di un elenco di sottoreti approvate. La regola è NON_COMPLIANT se un'istanza del notebook non viene avviata all'interno di un VPC o se il relativo ID di sottorete non è incluso nell'elenco dei parametri.

Identificatore: SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

Tipi di risorse: AWS::SageMaker::NotebookInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

SubnetIds (Facoltativo), Tipo: CSV

Elenco separato da virgole degli ID di sottorete in cui è possibile avviare le istanze del notebook.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

sagemaker-notebook-instance-kms-key-configured

Verifica se una AWS chiave Key Management Service (AWS KMS) è configurata per un'istanza di SageMaker notebook Amazon. La regola è NON_COMPLIANT se non è specificato 'KmsKeyId' per l'istanza del notebook. SageMaker

Identificatore: SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED

Tipi di risorse: AWS::SageMaker::NotebookInstance

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsKeyArns (Facoltativo), ▬Tipo: stringa

Elenco separato da virgole di ARN di chiavi AWS KMS consentite per un'istanza di notebook Amazon. SageMaker

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

sagemaker-notebook-instance-root-access-check

Verifica se l' SageMaker RootAccess impostazione Amazon è abilitata per le istanze di SageMaker notebook Amazon. La regola è NON_COMPLIANT se l' RootAccess impostazione è impostata su «Enabled» per un'istanza Amazon Notebook. SageMaker

Identificatore: SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

Tipi di risorse: AWS::SageMaker::NotebookInstance

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

sagemaker-notebook-no-direct-internet-access

Verifica se l'accesso diretto a Internet è disabilitato per un'istanza di SageMaker notebook Amazon. La regola è NON_COMPLIANT se un'istanza di SageMaker notebook è abilitata a Internet.

Identificatore: SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

Tipi di risorse: AWS::SageMaker::NotebookInstance

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

secretsmanager-rotation-enabled-check

Verifica se il segreto di AWS Secrets Manager ha la rotazione abilitata. La regola controlla anche un parametro `maximumAllowedRotationFrequency` facoltativo. Se il parametro è specificato, la frequenza di rotazione del segreto viene confrontata con la frequenza massima consentita. La regola è NON_COMPLIANT se il segreto non è pianificato per la rotazione. La regola è anche NON_COMPLIANT se la frequenza di rotazione è superiore al numero specificato nel parametro Frequency. maximumAllowedRotation

> **Note**
> Rivalutare questa regola entro 4 ore dalla prima valutazione non avrà effetto sui risultati.

Identificatore: SECRETSMANAGER_ROTATION_ENABLED_CHECK

Tipi di risorse: AWS::SecretsManager::Secret

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

massimo AllowedRotationFrequency (opzionale), Tipo: int

Frequenza massima consentita di rotazione del segreto in giorni.

massimo AllowedRotationFrequencyInHours (opzionale), Tipo: int

Frequenza massima consentita di rotazione del segreto in ore.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

secretsmanager-scheduled-rotation-success-check

Verifica se AWS i segreti di Secrets Manager sono stati ruotati correttamente in base al programma di rotazione. Secrets Manager calcola la data in cui dovrebbe avvenire la rotazione. La regola è NON_COMPLIANT se la data è trascorsa e il segreto non è stato ruotato.

> **Note**
> La regola restituisce NOT_APPLICABLE per i segreti senza rotazione.

Identificatore: SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK

Tipi di risorse: AWS::SecretsManager::Secret

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

secretsmanager-secret-periodic-rotation

Verifica se AWS i segreti di Secrets Manager sono stati ruotati nell'ultimo numero di giorni specificato. La regola è NON_COMPLIANT se un segreto non è stato ruotato per più di un numero di giorni di rotazione. maxDaysSince Il valore predefinito è 90 giorni.

Identificatore: SECRETSMANAGER_SECRET_PERIODIC_ROTATION

Tipi di risorse: AWS::SecretsManager::Secret

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

max DaysSinceRotation (opzionale), Tipo: int

> Numero massimo di giorni in cui un segreto può rimanere invariato. Il valore predefinito è 90 giorni.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

secretsmanager-secret-unused

Verifica se AWS è stato effettuato l'accesso ai segreti di Secrets Manager entro un determinato numero di giorni. La regola è NON_COMPLIANT se non è stato effettuato l'accesso a un segreto per un numero di giorni «ForDaysinutilizzato». Il valore predefinito è 90 giorni.

Contesto: si consiglia di eliminare regolarmente i segreti non utilizzati. I segreti non utilizzati possono essere usati in modo improprio dagli ex utenti che non hanno più bisogno di accedervi. Inoltre, man mano che sempre più utenti accedono a un segreto, diventa sempre più probabile che qualcuno lo abbia utilizzato in modo improprio o che abbia concesso l'accesso a un'entità non autorizzata. L'eliminazione dei segreti inutilizzati aiuta a revocarne l'accesso agli utenti che non ne hanno più bisogno e può ridurre i costi di utilizzo di AWS Secrets Manager.

Identificatore: SECRETSMANAGER_SECRET_UNUSED

Tipi di risorse: AWS::SecretsManager::Secret

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

unusedForDays (Facoltativo), Tipo: int

> Il numero massimo di giorni in cui un segreto può rimanere inutilizzato. Il valore predefinito è 90 giorni.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

secretsmanager-using-cmk

Verifica se tutti i segreti in AWS Secrets Manager ingresso sono crittografati utilizzando Chiave gestita da AWS (`aws/secretsmanager`) o una chiave gestita dal cliente creata in AWS Key Management Service (AWS KMS). La regola è COMPLIANT se un segreto è crittografato utilizzando una chiave gestita dal cliente. Questa regola è NON_COMPLIANT se un segreto è crittografato utilizzando `aws/secretsmanager`.

> **Note**
>
> Questa regola non ha accesso alle chiavi gestite dai clienti su più account e valuta i segreti come NON_COMPLIANT quando viene utilizzata una chiave per più account.

Identificatore: SECRETSMANAGER_USING_CMK

Tipi di risorse: AWS::SecretsManager::Secret

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsKeyArns (Facoltativo), Tipo: CSV

Elenco separato da virgole dei nomi della risorsa Amazon (ARN) delle chiavi KMS per verificare se le chiavi sono utilizzate nella crittografia.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

securityhub-enabled

Verifica se AWS Security Hub è abilitato per un AWS account. La regola è NON_COMPLIANT se AWS Security Hub non è abilitato.

Identificatore: SECURITYHUB_ENABLED

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

security-account-information-provided

Verifica se hai fornito informazioni di contatto di sicurezza per i contatti AWS del tuo account. La regola è NON_COMPLIANT se non sono state fornite le informazioni di contatto di sicurezza all'interno dell'account.

Identificatore: SECURITY_ACCOUNT_INFORMATION_PROVIDED

Tipi di risorse: AWS::::Account

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

catalogo dei servizi condiviso all'interno dell'organizzazione

Verifica se AWS Service Catalog condivide i portafogli con un'organizzazione (una raccolta di AWS account considerati come una singola unità) quando l'integrazione è abilitata con AWS Organizations. La regola è NON_COMPLIANT se il valore `Type` di una condivisione è `ACCOUNT`.

Identificatore: SERVICE_CATALOG_SHARED_WITHIN_ORGANIZATION

Tipi di risorse: AWS::ServiceCatalog::Portfolio

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

service-vpc-endpoint-enabled

Verifica se per ogni Amazon Virtual Private Cloud (Amazon VPC) viene creato un endpoint di servizio per il servizio fornito nel parametro della regola. La regola è NON_COMPLIANT se un Amazon VPC non dispone di un endpoint Amazon VPC creato per il servizio.

Identificatore: SERVICE_VPC_ENDPOINT_ENABLED

Tipi di risorse: AWS: :EC2: :VPC

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

serviceName, ▪Tipo: stringa

Il nome breve o il suffisso del servizio. Nota: per ottenere un elenco di nomi di servizio disponibili o un elenco di suffissi validi, usa DescribeVpcEndpointServices.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ses-malware-scanning-enabled

Verifica se la scansione di malware e spam sui messaggi in entrata è abilitata per Amazon Simple Email Service (Amazon SES). La regola è NON_COMPLIANT se la scansione di malware e spam non è abilitata.

Identificatore: SES_MALWARE_SCANNING_ENABLED

Tipi di risorse: AWS::SES::ReceiptRule

Tipo di trigger: Periodico

Regione AWS: disponibile soltanto nelle regioni Europa (Irlanda), Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

shield-advanced-enabled-autorenew

Verifica se AWS Shield Advanced è abilitato nel tuo AWS account e questo abbonamento è impostato per il rinnovo automatico. La regola è COMPLIANT se Shield Advanced è abilitato e se il rinnovo automatico è abilitato.

> **Note**
>
> L'endpoint API di AWS Shield Advanced è disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale). Questa regola deve essere pianificata per l'esecuzione solo nella regione Stati Uniti orientali (Virginia settentrionale).

Identificatore: SHIELD_ADVANCED_ENABLED_AUTORENEW

Tipo di trigger: Periodico

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

shield-drt-access

Verifica se lo Shield Response Team (SRT) può accedere al tuo AWS account. La regola è NON_COMPLIANT se AWS Shield Advanced è abilitata ma il ruolo per l'accesso SRT non è configurato.

Identificatore: SHIELD_DRT_ACCESS

Tipo di trigger: Periodico

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

sns-encrypted-kms

Verifica se gli argomenti SNS sono crittografati con AWS Key Management Service (KMS).AWS La regola è NON_COMPLIANT se un argomento SNS non è crittografato con KMS. AWS Facoltativamente, specificare gli ARN delle chiavi, gli alias ARN, il nome dell'alias o gli ID delle chiavi per la regola da controllare.

Identificatore: SNS_ENCRYPTED_KMS

Tipi di risorse: AWS::SNS::Topic

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

kmsKeyIds (Facoltativo), Tipo: CSV

Elenco separato da virgole di chiavi AWS KMS Amazon Resource Names (ARN), alias ARN KMS, nomi alias KMS o ID chiave KMS da verificare per la regola.

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with Rules. AWS Config Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
   "KmsMasterKeyId": "my-kms-key-Id"
}
...
```

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

sns-topic-message-delivery-notification-enabled

Verifica se la registrazione di log di Amazon Simple Notification Service (SNS) è abilitata per lo stato di consegna dei messaggi di notifica inviati a un argomento per gli endpoint. La regola è NON_COMPLIANT se la notifica dello stato di consegna dei messaggi non è abilitata.

Identificatore: SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

Tipi di risorse: AWS::SNS::Topic

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

ssm-document-not-public

Verifica se AWS i documenti di Systems Manager di proprietà dell'account sono pubblici. La regola è NON_COMPLIANT se i documenti di Systems Manager con il proprietario "Self" sono pubblici.

Identificatore: SSM_DOCUMENT_NOT_PUBLIC

Tipi di risorse: AWS::SSM::Document

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

step-functions-state-machine-logging-enabled

Verifica se la macchina AWS Step Functions ha la registrazione abilitata. La regola è NON_COMPLIANT se la registrazione di log non è abilitata per una macchina a stati o se la configurazione della registrazione di log non è al livello minimo fornito.

Identificatore: STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

Tipi di risorse: AWS::StepFunctions::StateMachine

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

cloud WatchLogGroupArns (opzionale), Tipo: CSV

Elenco separato da virgole di Amazon Resource Names (ARN) per i gruppi di log Amazon CloudWatch Logs. La regola verifica se i gruppi di log specificati sono configurati per i log della macchina a stati in uso.

logLevel (opzionale), -Tipo: stringa

Il livello di log minimo per la macchina a stati. I valori validi includono: ALL, ERROR, FATAL.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

storagegateway-last-backup-recovery-point-created

Verifica se è stato creato un punto di ripristino per i volumi AWS Storage Gateway. La regola è NON_COMPLIANT se il volume Storage Gateway non dispone di un punto di ripristino corrispondente creato entro il periodo di tempo specificato.

Identificatore: STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipi di risorse: AWS::StorageGateway::Volume

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), -Tipo: stringa

Tag dei volumi Storage Gateway che la regola deve verificare, in formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opzionale), -Tipo: stringa

ID del volume Storage Gateway che la regola deve verificare.

ripristino PointAgeValue (opzionale), Tipo: int, Impostazione predefinita: 1

Valore numerico per la durata massima consentita. Non superiore a 744 per le ore e 31 per i giorni.

ripristino PointAgeUnit (opzionale), ▬Tipo: stringa, Impostazione predefinita: giorni

Unità di tempo per la durata massima consentita. Valori accettati: "ore", "giorni".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

storagegateway-resources-protected-by-backup-plan

Verifica se i volumi AWS di Storage Gateway sono protetti da un piano di backup. La regola è NON_COMPLIANT se il volume Storage Gateway non è coperto da un piano di backup.

Identificatore: STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipi di risorse: AWS::StorageGateway::Volume

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▬Tipo: stringa

Tag dei volumi Storage Gateway che la regola deve verificare, in formato JSON.

resourceId (opzionale), ▬Tipo: stringa

ID del volume Storage Gateway che la regola deve verificare.

crossRegionList (Facoltativo), ▬Tipo: stringa

Elenco separato da virgole delle regioni di destinazione della copia di backup tra regioni da conservare

crossAccountList (Opzionale), ▬Tipo: stringa

Elenco separato da virgole degli account di destinazione della copia di backup tra account da conservare

maxRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione massimo in giorni per Vault Lock di Backup

minRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione minimo in giorni per Vault Lock di Backup

backup VaultLockCheck (opzionale), ➖Tipo: stringa

Valori accettati: "True" o "False". Immetti "True" per fare in modo che la regola verifichi se per la risorsa viene eseguito il backup in un vault bloccato

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

subnet-auto-assign-public-ip-disabled

Verifica se alle sottoreti Amazon Virtual Private Cloud (Amazon VPC) viene assegnato un indirizzo IP pubblico. La regola è COMPLIANT se Amazon VPC non dispone di sottoreti a cui viene assegnato un indirizzo IP pubblico. La regola è NON_COMPLIANT se Amazon VPC dispone di sottoreti a cui viene assegnato un indirizzo IP pubblico.

Identificatore: SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

Tipi di risorse: AWS::EC2::Subnet

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

Valutazione proattiva

Per istruzioni su come eseguire questa regola in modalità proattiva, consulta Evaluating Your Resources with AWS Config Rules. Affinché questa regola restituisca COMPLIANT in modalità proattiva, lo schema di configurazione delle risorse per l'API di StartResourcevalutazione deve includere i seguenti input, codificati come stringa:

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

Per ulteriori informazioni sulla valutazione proattiva, consulta Modalità di valutazione.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

transfer-family-server-noftp

Verifica se un server creato con AWS Transfer Family utilizza FTP per la connessione agli endpoint. La regola è NON_COMPLIANT se il protocollo server per la connessione agli endpoint è abilitato all'FTP.

Identificatore: TRANSFER_FAMILY_SERVER_NO_FTP

Tipi di risorse: AWS::Transfer::Server

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

virtualmachine-last-backup-recovery-point-created

Verifica se è stato creato un punto di ripristino per AWS VirtualMachines Backup-Gateway. La regola è NON_COMPLIANT se un AWS Backup-Gateway VirtualMachines non dispone di un punto di ripristino corrispondente creato entro il periodo di tempo specificato.

Identificatore: VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipi di risorse: AWS::BackupGateway::VirtualMachine

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▬Tipo: stringa

Tag di AWS Backup-Gateway VirtualMachines per la regola da controllare, in formato JSON. `{"tagkey" : "tagValue"}`

resourceId (opzionale), ▬Tipo: stringa

ID di AWS Backup-Gateway VirtualMachine per la regola da verificare.

ripristino PointAgeValue (facoltativo), Tipo: int, Impostazione predefinita: 1

Valore numerico per la durata massima consentita. Non superiore a 744 per le ore e 31 per i giorni.

ripristino PointAgeUnit (opzionale), ▬Tipo: stringa, Impostazione predefinita: giorni

Unità di tempo per la durata massima consentita. Valori accettati: "ore", "giorni".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

virtualmachine-resources-protected-by-backup-plan

Verifica se i AWS Backup-Gateway VirtualMachines sono protetti da un piano di backup. La regola è NON_COMPLIANT se il Backup-Gateway non VirtualMachine è coperto da un piano di backup.

Identificatore: VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipi di risorse: AWS::BackupGateway::VirtualMachine

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

resourceTags (opzionale), ▪Tipo: stringa

Tag per AWS Backup-Gateway VirtualMachines per la regola da controllare, in formato JSON. `{"tagkey" : "tagValue"}`

resourceId (opzionale), ▪Tipo: stringa

ID di AWS Backup-Gateway VirtualMachine per la regola da verificare.

crossRegionList (Facoltativo), ▪Tipo: stringa

Elenco separato da virgole delle regioni di destinazione della copia di backup tra regioni da conservare

crossAccountList (Opzionale), ▪Tipo: stringa

Elenco separato da virgole degli account di destinazione della copia di backup tra account da conservare

maxRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione massimo in giorni per Vault Lock di Backup

minRetentionDays (Opzionale), Tipo: int

Il periodo di conservazione minimo in giorni per Vault Lock di Backup

backup VaultLockCheck (opzionale), ▪Tipo: stringa

Valori accettati: "True" o "False". Immetti "True" per fare in modo che la regola verifichi se per la risorsa viene eseguito il backup in un vault bloccato

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

vpc-default-security-group-closed

Verifica se il gruppo di sicurezza predefinito di qualsiasi Amazon Virtual Private Cloud (Amazon VPC) non consente il traffico in entrata o in uscita. La regola è NON_COMPLIANT se il gruppo di sicurezza predefinito ha una o più regole di traffico in entrata o in uscita.

> **Note**
>
> Potrebbe verificarsi un ritardo tra il momento in cui viene AWS Config registrata l'eliminazione di risorse correlate, come i gruppi di sicurezza predefiniti, che vengono eliminati come parte dell'eliminazione di Amazon VPC. Di conseguenza, anche se tutti i gruppi di sicurezza predefiniti o le altre risorse correlate sono stati eliminati o riparati, la regola può segnalare un risultato NON_COMPLIANT fino al successivo processo che stabilisce la linea di base dell'account.

Identifier (Identificatore): VPC_DEFAULT_SECURITY_GROUP_CLOSED

Tipi di risorse: AWS::EC2::SecurityGroup

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedere[Creazione di regole gestite di AWS Config con modelli AWS CloudFormation](#).

vpc-flow-logs-enabled

Verifica se i log di flusso di Amazon Virtual Private Cloud (Amazon VPC) sono stati trovati e sono abilitati per tutti i VPC Amazon. La regola è NON_COMPLIANT se i log di flusso non sono abilitati per almeno un VPC Amazon.

Identifier (Identificatore): VPC_FLOW_LOGS_ENABLED

Tipi di risorse: AWS: :EC2: :VPC

Tipo di trigger: Periodico

Regione AWS: Tutte le regioni supportate AWS

Parametri:

trafficType (opzionale), ▪Tipo: stringa

TrafficType dei registri di flusso

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

vpc-network-acl-unused-check

Verifica se sono presenti liste di controllo degli accessi alla rete (ACL di rete) non utilizzate. La regola è COMPLIANT se ogni ACL di rete è associata a una sottorete. La regola è NON_COMPLIANT se un'ACL di rete non è associata a una sottorete.

Identificatore: VPC_NETWORK_ACL_UNUSED_CHECK

Tipi di risorse: AWS::EC2::NetworkAcl

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

vpc-peering-dns-resolution-check

Verifica se la risoluzione DNS dal VPC dell'accettante/richiedente all'IP privato è abilitata. La regola è NON_COMPLIANT se la risoluzione DNS dal VPC dell'accettante/richiedente all'IP privato non è abilitata.

Identificatore: VPC_PEERING_DNS_RESOLUTION_CHECK

Tipi di risorse: AWS: :EC2: :VPC PeeringConnection

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

vpcIds (opzionale), Tipo: CSV

Elenco separato da virgole degli ID dei VPC da controllare.

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

vpc-sg-open-only-to-authorized-ports

Verifica se i gruppi di sicurezza che consentono il traffico in entrata senza restrizioni ("0.0.0.0/0" o "::/0") consentono solo connessioni TCP o UDP in entrata sulle porte autorizzate. La regola è NON_COMPLIANT se tali gruppi di sicurezza non dispongono di porte specificate nei parametri della regola.

> **Note**
>
> Questa regola valuta i gruppi di sicurezza Amazon EC2 con la regola di ingresso impostata su IPv4='0.0.0.0/0' o IPv6='::/'. Se il gruppo di sicurezza non ha una di queste destinazioni, questa regola restituisce `NOT_APPLICABLE`.

Identificatore: VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

Tipi di risorse: AWS::EC2::SecurityGroup

Tipo di trigger: Modifiche alla configurazione e periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

authorizedTcpPorts (Facoltativo), ▬Tipo: stringa

Elenco separato da virgole delle porte TCP autorizzate ad essere aperte a 0.0.0.0/0 o ::/0. Gli intervalli sono definiti dal trattino, ad esempio "443.1020-1025".

authorizedUdpPorts (Opzionale), ▬Tipo: stringa

Elenco separato da virgole delle porte UDP autorizzate ad essere aperte a 0.0.0.0/0 o ::/0. Gli intervalli sono definiti dal trattino, ad esempio "500.1020-1025".

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

controllo della restrizione della porta vpc-sg-

Verifica se i gruppi di sicurezza limitano il traffico in entrata alle porte con restrizioni in modo esplicito a partire da 0.0.0.0/0 o: :/0. La regola è NON_COMPLIANT se i gruppi di sicurezza consentono il traffico in entrata da 0.0.0.0/0 o: :/0 sulle porte TCP/UDP 22/3389 o come specificato nei parametri.

Identificatore: VPC_SG_PORT_RESTRICTION_CHECK

Tipi di risorse: AWS::EC2::SecurityGroup

Tipo di trigger: Periodico

Regione AWS: Tutte le AWS regioni supportate

Parametri:

RestrictPorts (opzionale), Tipo: CSV

Elenco separato da virgole di porte che non devono essere aperte al traffico in entrata sull'intero intervallo IP. I numeri di porta validi sono compresi tra 0 e 65535. Se non viene specificato, per impostazione predefinita la regola controlla 22 e 3389.

Tipo di protocollo (opzionale), ▬Tipo: stringa

Il tipo di protocollo di trasmissione per la regola da controllare. I valori validi includono 'TCP', 'UDP' e 'ALL' (senza distinzione tra maiuscole e minuscole). Se impostata su 'ALL', la regola verificherà le regole che utilizzano il protocollo 'TCP', 'UDP' o 'ALL' (-1). Il valore predefinito è «ALL'».

escludere ExternalSecurityGroups (facoltativo), Tipo: booleano

Contrassegno booleano per escludere la valutazione di gruppi di sicurezza esterni. Se impostata su «true», la regola non includerà gruppi di sicurezza esterni nella valutazione. Altrimenti, tutti

i gruppi di sicurezza vengono valutati se il valore è impostato su «false». Il valore predefinito è 'true'.

IPType (opzionale), ▪Tipo: stringa

La versione IP (Internet Protocol) della regola da verificare. I valori validi includono 'IPv4', 'IPv6' e 'ALL' (senza distinzione tra maiuscole e minuscole). Se non viene specificato, per impostazione predefinita la regola controlla «TUTTI».

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

vpc-vpn-2-tunnels-up

Verifica se entrambi i tunnel di rete privata virtuale (VPN) forniti da AWS Site-to-Site VPN sono nello stato UP. La regola è NON_COMPLIANT se uno o entrambi i tunnel sono nello stato DOWN.

Identificatore: VPC_VPN_2_TUNNELS_UP

Tipi di risorse: AWS::EC2::VPNConnection

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

wafv2-logging-enabled

Verifica se la registrazione è abilitata negli elenchi di controllo di accesso Web regionali e globali AWS WAFv2 (ACL Web). La regola è NON_COMPLIANT se la registrazione di log è abilitata, ma la destinazione della registrazione non corrisponde al valore del parametro.

Identificatore: WAFV2_LOGGING_ENABLED

Tipi AWS::WAFv2::Web di risorse: ACL

Tipo di trigger: Periodico

Regione AWS: tutte le regioni supportate AWS

Parametri:

KinesisFirehoseDeliveryStreamArns (Facoltativo), Tipo: CSV

Elenco separato da virgole degli ARN del flusso di consegna di Kinesis Firehose

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

wafv2-rulegroup-logging-enabled

Verifica se la raccolta dei parametri CloudWatch di sicurezza di Amazon sui gruppi di regole AWS WAFv2 è abilitata. La regola è NON_COMPLIANT se '. VisibilityConfig CloudWatchMetricsEnabled'il campo è impostato su false.

Contesto: AWS WAFV2 (Web Application Firewall versione 2) consente di creare AWS WAF regole per proteggere le applicazioni Web da exploit e vulnerabilità Web comuni. Un gruppo di AWS WAF regole è una raccolta di AWS WAF regole che è possibile associare a un ACL (Access Control List) Web per definire il comportamento desiderato per il traffico delle applicazioni Web. Per ulteriori informazioni, consulta AWS WAF le regole e i gruppi di regole nella Guida per gli AWS WAF sviluppatori.

Configurando la raccolta dei parametri di CloudWatch sicurezza nel gruppo di AWS WAFV2 regole, puoi monitorare parametri di sicurezza come gli attacchi Distributed Denial of Service (DDoS), SQL injection e Cross-site Scripting (XSS) riusciti o falliti. Le metriche di sicurezza raccolte possono aiutarti a semplificare le indagini.

> **Note**
>
> Se non ci sono AWS WAF regole nel gruppo di regole da verificare per la AWS WAFV2 regola AWS Config gestita, la regola gestita restituisce NON_APPLICABLE AWS Config .

Identificatore: WAFV2_RULEGROUP_LOGGING_ENABLED

Tipi di risorse: AWS::WAFv2::RuleGroup

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

wafv2-rulegroup-not-empty

Verifica se i gruppi di regole WAFv2 contengono regole. La regola è NON_COMPLIANT se non ci sono regole presenti all'interno di un gruppo di regole WAFv2.

Identificatore: WAFV2_RULEGROUP_NOT_EMPTY

Tipi di risorse: AWS::WAFv2::RuleGroup

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

wafv2-webacl-not-empty

Verifica se un'ACL Web WAFv2 contiene regole o gruppi di regole WAF. Questa regola è NON_COMPLIANT se un'ACL Web non contiene alcuna regola o gruppo di regole WAF.

Identificatore: WAFV2_WEBACL_NOT_EMPTY

Tipi di risorse: AWS::WAFv2::Web ACL

Tipo di trigger: Modifiche alla configurazione

Regione AWS: tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

waf-classic-logging-enabled

Verifica se la registrazione è abilitata nelle classiche liste di controllo degli accessi web globali AWS (ACL web) di WAF classic. La regola è NON_COMPLIANT se la registrazione di log non è abilitata per un'ACL Web globale.

Identificatore: WAF_CLASSIC_LOGGING_ENABLED

Tipi di risorse: ACL AWS::WAF::Web

Tipo di trigger: Periodico

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

KinesisFirehoseDeliveryStreamArns (Facoltativo), Tipo: CSV

Elenco separato da virgole di Amazon Kinesis stream ARN per i log WAF. AWS

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

waf-global-rulegroup-not-empty

Verifica se un gruppo di regole AWS WAF Classic contiene delle regole. La regola è NON_COMPLIANT se non ci sono regole presenti all'interno di un gruppo di regole.

Identificatore: WAF_GLOBAL_RULEGROUP_NOT_EMPTY

Tipi di risorse: AWS::WAF::RuleGroup

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

waf-global-rule-not-empty

Verifica se una regola globale AWS WAF contiene delle condizioni. La regola è NON_COMPLIANT se non sono presenti condizioni all'interno della regola globale WAF.

Identificatore: WAF_GLOBAL_RULE_NOT_EMPTY

Tipi di risorse: AWS::WAF::Rule

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

waf-global-webacl-not-empty

Verifica se un'ACL Web WAF Global contiene regole o gruppi di regole WAF. Questa regola è NON_COMPLIANT se un'ACL Web non contiene alcuna regola o gruppo di regole WAF.

Identificatore: WAF_GLOBAL_WEBACL_NOT_EMPTY

Tipi di risorse: AWS::WAF::Web ACL

Tipo di trigger: Modifiche alla configurazione

Regione AWS: disponibile solo nella regione Stati Uniti orientali (Virginia settentrionale)

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

waf-regional-rulegroup-not-empty

Verifica se i gruppi di regole regionali WAF contengono regole. La regola è NON_COMPLIANT se non ci sono regole presenti all'interno di un gruppo di regole regionali WAF.

Identificatore: WAF_REGIONAL_RULEGROUP_NOT_EMPTY

Tipi di risorse: AWS::WAFRegional::RuleGroup

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

waf-regional-rule-not-empty

Verifica se la regola regionale WAF contiene condizioni. Questa regola è COMPLIANT se la regola regionale contiene almeno una condizione e NON_COMPLIANT in caso contrario.

Identificatore: WAF_REGIONAL_RULE_NOT_EMPTY

Tipi di risorse: AWS::WAFRegional::Rule

Tipo di trigger: Modifiche alla configurazione

Regione AWS: Tutte le AWS regioni supportate

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

waf-regional-webacl-not-empty

Verifica se un'ACL Web regionale WAF contiene regole o gruppi di regole WAF. La regola è NON_COMPLIANT se non ci sono regole o gruppi di regole WAF all'interno di un'ACL Web.

Identificatore: WAF_REGIONAL_WEBACL_NOT_EMPTY

Tipi di risorse: AWS::WAFRegional::Web ACL

Tipo di trigger: Modifiche alla configurazione

Regione AWS: tutte le regioni supportate AWS

Parametri:

Nessuno

AWS CloudFormation modello

Per creare regole AWS Config gestite con AWS CloudFormation modelli, vedereCreazione di regole gestite di AWS Config con modelli AWS CloudFormation.

Elenco di regole AWS Config gestite per modalità di valutazione

AWS Config attualmente supporta le seguenti regole gestite.

Considerazioni

Valori predefiniti per le regole gestite

I valori predefiniti specificati per le regole gestite sono precompilati solo quando si utilizza la console. AWS I valori predefiniti non sono forniti per l'API, la CLI o l'SDK.

I bucket di directory non sono supportati

Le regole gestite supportano solo bucket generici durante la valutazione delle risorse di Amazon Simple Storage Service (Amazon S3). AWS Config non registra le modifiche alla configurazione per i bucket di directory. Per ulteriori informazioni sui bucket generici e sui bucket di directory, consulta la panoramica dei bucket e bucket di directory nella guida utente di Amazon S3.

Regole gestite e tipi di risorse IAM globali

I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.

Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.

Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.

Valutazione proattiva

Le regole proattive sono regole che supportano la modalità di valutazione proattiva per le risorse che non sono state implementate. Ciò consente di valutare se un insieme di proprietà delle risorse, se utilizzato per definire una AWS risorsa, sarebbe CONFORME o NON CONFORME, in base

all'insieme di regole proattive che hai nel tuo account nella tua regione. Per ulteriori informazioni, consulta Modalità di valutazione.

> **Note**
>
> Le regole proattive non correggono le risorse contrassegnate come NON_COMPLIANT e non ne impediscono l'implementazione.

Valutazione proattiva

- api-gw-xray-enabled
- autoscaling-group-elb-healthcheck-required
- ec2-instance-multiple-eni-check
- eip-attached
- elasticsearch-node-to-node-encryption-check
- lambda-function-settings-check
- lambda-inside-vpc
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-public-access-check
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- s3-bucket-logging-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled

Valutazione di test

Le regole di test sono regole che supportano la modalità di valutazione di test per le risorse che sono già state implementate. Ciò consente di valutare le impostazioni di configurazione delle risorse esistenti.

> **Note**
>
> Attualmente, tutte le regole supportano la valutazione investigativa. AWS Config

Valutazione di test

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created

- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check

- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check

- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic

- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version

- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access

- iam-role-managed-policy-check
- iam-root-access-key-check
- controllo della scadenza del certificato iam-server
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- abilitato a inspector-ec2-scan
- abilitato a inspector-ecr-scan
- abilitato a inspector-lambda-code-scan-scan
- abilitato a inspector-lambda-standard-scan
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled

- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required

- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled

- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo della restrizione della porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Elenco di regole AWS Config gestite per tipo di trigger

AWS Config attualmente supporta le seguenti regole gestite.

Considerazioni

Valori predefiniti per le regole gestite

I valori predefiniti specificati per le regole gestite sono precompilati solo quando si utilizza la console. AWS I valori predefiniti non sono forniti per l'API, la CLI o l'SDK.

I bucket di directory non sono supportati

Le regole gestite supportano solo bucket generici durante la valutazione delle risorse di Amazon Simple Storage Service (Amazon S3). AWS Config non registra le modifiche alla configurazione per i bucket di directory. Per ulteriori informazioni sui bucket generici e sui bucket di directory, consulta la panoramica dei bucket e bucket di directory nella guida utente di Amazon S3.

Regole gestite e tipi di risorse IAM globali

I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.

Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.

Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate. Per un elenco delle regole gestite supportate in quali regioni, consulta Elenco delle regole AWS Config gestite per disponibilità regionale.

Modifiche della configurazione

Le regole attivate dalle modifiche sono regole che vengono AWS Config valutate in risposta alle modifiche alla configurazione.

Modifiche della configurazione

- acm-certificate-rsa-check
- alb-desync-mode-check

- alb-http-drop-invalid-header-enabled
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az

- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-settings-check
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db-abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- ebs-optimized-instance
- ec2-client-vpn-connection-log-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted

- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-supported-version
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch

- elastic-beanstalk-managed-updates-enabled
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- global-endpoint-event-replication-enabled
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-user-group-membership-check
- iam-user-no-policies-check
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited

- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance

- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled

- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica tra più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-using-cmk
- catalogo di servizi condiviso all'interno dell'organizzazione
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Periodic (Periodico)

Le regole periodiche sono regole che vengono AWS Config valutate periodicamente con una frequenza specificata dall'utente, ad esempio ogni 24 ore.

Periodic (Periodico)

- access-keys-rotated
- account-part-of-organizations
- acm-pca-root-ca-disabled

- alb-http-to-https-redirection-check
- api-gwv2-authorization-type-configured
- appsync-associated-with-waf
- appsync-cache-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- cloudfront-s3-origin-non-existent-bucket
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target

- dynamodb-resources-protected-by-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-last-backup-recovery-point-created
- ec2-meets-restore-time-target
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ecr-private-image-scanning-enabled
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eks-cluster-logging-enabled
- eks-cluster-secrets-criptato
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest

- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2-acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- sono abilitato all'analizzatore di accesso esterno
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- controllo della scadenza del certificato iam-server
- iam-user-mfa-enabled

- iam-user-unused-credentials-check
- abilitato a inspector-ec2-scan
- abilitato a inspector-ecr-scan
- abilitato a inspector-lambda-code-scan-scan
- abilitato a inspector-lambda-standard-scan
- kinesis-firehose-delivery-stream crittografato
- kms-cmk-not-scheduled-for-deletion
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-automatic-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- multi-region-cloud-trail-enabled
- netfw-logging-enabled
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-resources-protected-by-backup-plan
- redshift - accesso illimitato alle porte
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-account-level-public-access-blocks-periodic
- s3-last-backup-recovery-point-created
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-flow-logs-enabled
- controllo di restrizione delle porte vpc-sg-
- wafv2-logging-enabled
- waf-classic-logging-enabled

Ibrido

Le regole ibride sono regole che vengono valutate sia in risposta alle modifiche di configurazione che periodicamente AWS Config .

Ibrido

- acm-certificate-expiration-check
- cloudformation-stack-drift-detection-check
- incoming-ssh-disabled
- restricted-incoming-traffic
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

Elenco delle regole AWS Config gestite per disponibilità regionale

AWS Config attualmente supporta le seguenti regole gestite.

Considerazioni

Valori predefiniti per le regole gestite

I valori predefiniti specificati per le regole gestite sono precompilati solo quando si utilizza la console. AWS I valori predefiniti non sono forniti per l'API, la CLI o l'SDK.

I bucket di directory non sono supportati

Le regole gestite supportano solo bucket generici durante la valutazione delle risorse di Amazon Simple Storage Service (Amazon S3). AWS Config non registra le modifiche alla configurazione per i bucket di directory. Per ulteriori informazioni sui bucket generici e sui bucket di directory, consulta la panoramica dei bucket e bucket di directory nella guida utente di Amazon S3.

Regole gestite e tipi di risorse IAM globali

I tipi di risorse IAM globali inseriti prima di febbraio 2022 (`AWS::IAM::Group`, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) possono essere registrati solo AWS nelle regioni AWS Config in cui AWS Config erano disponibili prima di febbraio 2022. Questi tipi di risorse non possono essere registrati nelle regioni supportate AWS Config dopo febbraio 2022. Per un elenco di tali regioni, consulta AWS Risorse di registrazione | Risorse globali.

Se registri un tipo di risorsa IAM globale in almeno una regione, le regole periodiche che segnalano la conformità sul tipo di risorsa IAM globale eseguiranno valutazioni in tutte le regioni in cui viene aggiunta la regola periodica, anche se non hai abilitato la registrazione del tipo di risorsa IAM globale nella regione in cui è stata aggiunta la regola periodica.

Per evitare valutazioni non necessarie, dovresti distribuire regole periodiche che segnalino la conformità su un tipo di risorsa IAM globale solo in una delle regioni supportate.

Stati Uniti orientali (Ohio)

Stati Uniti orientali (Ohio)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check

- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan

- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- abilitato a inspector-lambda-code-scan-scan
- abilitato a inspector-lambda-standard-scan
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check

- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty

- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled

- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Stati Uniti orientali (Virginia settentrionale)

Stati Uniti orientali (Virginia settentrionale)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check

- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled

- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target

- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- controllo della scadenza del certificato iam-server-
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled

- abilitato a inspector-ec2-scan
- abilitato a inspector-ecr-scan
- abilitato a inspector-lambda-code-scan-scan
- abilitato a inspector-lambda-standard-scan
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check

- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable

- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl

- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target

- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan

- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Stati Uniti occidentali (California settentrionale)

Stati Uniti occidentali (California settentrionale)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled

- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled

- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured

- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check

- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes

- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check

- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls

- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check

- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check

- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check

- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled

- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Stati Uniti occidentali (Oregon)

US West (Oregon)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check

- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check

- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created

- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled

- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check

- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check

- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- abilitato a inspector-lambda-code-scan-scan
- abilitato a inspector-lambda-standard-scan
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled

- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance

- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check

- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled

- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Africa (Città del Capo)

Africa (Città del Capo)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- abilitato a dms-redis-tls
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled

- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic

- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan

- fsx-windows-audit-log-configured
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato

- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-public-access-check
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled

- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled

- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled

- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Asia Pacifico (Hong Kong)

Asia Pacifico (Hong Kong)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled

- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket

- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured

- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached

- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check

- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch

- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds

- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check

- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets

- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target

- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled

- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Asia Pacifico (Hyderabad)

Asia Pacific (Hyderabad)

- acm-certificate-expiration-check
- acm-pca-root-ca-disabled

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-mount-target-accessibile al pubblico
- eip-attached

- eks-cluster-log-enabled
- eks-cluster-secrets-criptato
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- guardduty-s3 abilitato alla protezione
- sono abilitato all'analizzatore di accesso esterno

- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- kinesis-firehose-delivery-stream crittografato
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited

- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check

- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

Regione Asia Pacifico (Giacarta)

Asia Pacifico (Giacarta)

- access-keys-rotated
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-encrypted-at-rest
- autoscaling-group-elb-healthcheck-required
- autoscaling-multiple-az
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check

- efs-mount-target-accessibile al pubblico
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-criptato
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-supported-engine-version
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime

- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- kinesis-firehose-delivery-stream crittografato
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc

- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-rabbit-deployment-mode
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-cluster-configuration-check

- redshift-cluster-maintenancesettings-check
- redshift-default-admin-check
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

Regione Asia Pacifico (Melbourne)

Asia Pacifico (Melbourne)

- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted

- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- cw-loggroup-retention-period-check

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- efs-mount-target-accessibile al pubblico
- eip-attached

- eks-cluster-secrets-criptato
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- guardduty-s3 abilitato alla protezione
- sono abilitato all'analizzatore di accesso esterno
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato

- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags

- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Asia Pacifico (Mumbai)

Asia Pacifico (Mumbai)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check

- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms

- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic

- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato

- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check

- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode

- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check

- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check

- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled

- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan

- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Asia Pacifico (Osaka-Locale)

Asia Pacifico (Osaka-Locale)

- access-keys-rotated
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest

- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-desync-mode-check
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled

- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- abilitato a dms-redis-tls
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-launch-template-public-ip-disabled
- ec2-no-amazon-key-pair
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecs-containers-readonly-access
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-mount-target-accessibile al pubblico
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled

- eks-cluster-secrets-criptato
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-supported-engine-version
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elbv2-multiple-az
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds

- abilitato alla protezione guardduty-s3
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-function-public-access-prohibited
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-cluster-default-admin-check
- rds-cluster-encrypted-at-rest
- rds-instance-default-admin-check
- rds-instance-public-access-check
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift - accesso illimitato alle porte

- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-peering-dns-resolution-check
- controllo di restrizione delle porte vpc-sg-
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Asia Pacifico (Seoul)

Asia Pacifico (Seoul)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check

- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check

- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes

- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check

- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled

- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance

- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check

- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created

- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Asia Pacifico (Singapore)

Asia Pacifico (Singapore)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check

- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check

- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached

- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check

- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes

- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check

- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- abilitato a inspector-lambda-code-scan-scan
- abilitato a inspector-lambda-standard-scan
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode

- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check

- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Asia Pacifico (Sydney)

Asia Pacifico (Sydney)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check

- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check

- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic

- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version

- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access

- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- abilitato a inspector-lambda-code-scan-scan
- abilitato a inspector-lambda-standard-scan
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log

- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only

- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled

- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Asia Pacifico (Tokyo)

Asia Pacifico (Tokyo)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled

- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check

- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled

- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled

- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan

- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled

- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only

- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use

- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- abilitato a inspector-lambda-code-scan-scan
- abilitato a inspector-lambda-standard-scan
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled

- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest

- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created

- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Canada (Centrale)

Canada (Centrale)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check

- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted

- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled

- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled

- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni

- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled

- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access

- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access

- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log

- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only

- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled

- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled

- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp

- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Canada occidentale (Calgary)

Canada occidentale (Calgary)

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- approved-amis-by-id
- approved-amis-by-tag
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-encryption-enabled
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- eip-attached
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- encrypted-volumes
- incoming-ssh-disabled
- instances-in-vpc
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled

- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

Regione Cina (Pechino)

Cina (Pechino)

- access-keys-rotated
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az

- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-s3-origin-non-existent-bucket
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public

- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured

- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled

- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check

- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited

- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica tra più regioni con bucket s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled

- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Cina (Ningxia)

Cina (Ningxia)

- access-keys-rotated

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check

- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public

- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance

- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled

- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check

- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato alla replica con s3-bucket in più regioni
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- controllo delle restrizioni delle porte vpc-sg-port

- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Europa (Francoforte)

Europa (Francoforte)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest

- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check

- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured

- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit

- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan

- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- abilitato a inspector-lambda-code-scan-scan

- abilitato a inspector-lambda-standard-scan
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled

- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest

- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Europa (Irlanda)

Europa (Irlanda)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled

- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target

- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato

- abilitato a inspector-ecr-scan
- abilitato a inspector-lambda-code-scan-scan
- abilitato a inspector-lambda-standard-scan
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check

- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte

- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check

- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check

- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Europa (Londra)

Europa (Londra)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled

- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check

- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured

- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created

- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check

- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- abilitato a inspector-lambda-code-scan-scan
- abilitato a inspector-lambda-standard-scan
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp

- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled

- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl

- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan

- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check

- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Europa (Milano)

Europa (Milano)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check

- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check

- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- abilitato a dms-redis-tls
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled

- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair

- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato

- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc

- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty

- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled

- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check

- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty

- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Europa (Parigi)

Europa (Parigi)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled

- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized

- abilitato alla protezione lambda guardduty
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled

- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited

- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Europa (Spagna)

Europa (Spagna)

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-mount-target-accessibile al pubblico
- eip-attached
- eks-cluster-log-enabled

- eks-cluster-secrets-criptato
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elbv2-multiple-az
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- guardduty-s3 abilitato alla protezione
- sono abilitato all'analizzatore di accesso esterno
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kinesis-firehose-delivery-stream crittografato
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- rds-instance-default-admin-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-mfa-delete-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- ssm-document-not-public

- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

Regione Europa (Stoccolma)

Europa (Stoccolma)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id

- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted

- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity

- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required

- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3

- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- abilitato a inspector-lambda-code-scan-scan
- abilitato a inspector-lambda-standard-scan
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check

- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets

- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled

- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited

- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Europa (Zurigo)

Europa (Zurigo)

- account-part-of-organizations

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-mount-target-accessibile al pubblico
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-criptato
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elbv2-multiple-az
- elb-deletion-protection-enabled
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime

- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- guardduty-s3 abilitato alla protezione
- sono abilitato all'analizzatore di accesso esterno
- iam-password-policy
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check

- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-snapshot-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

Regione di Israele (Tel Aviv)

Israele (Tel Aviv)

- account-part-of-organizations

- alb-desync-mode-check
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- eip-attached
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elb-cross-zone-load-balancing-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-eks-protection-audit-abilitato
- abilitato a guardduty-eks-protection-runtime
- abilitato alla protezione lambda guardduty
- guardduty-abilitato alla protezione da malware
- guardduty-s3 abilitato alla protezione
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- macie-auto-sensitive-data-discovery-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- controllo di restrizione delle porte vpc-sg-
- wafv2-webacl-not-empty

Regione Medio Oriente (Bahrein)

Medio Oriente (Bahrein)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled

- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check

- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached

- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets

- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- abilitato alla protezione lambda guardduty
- guardduty-abilitato alla protezione da malware

- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled

- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-rest
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public

- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Regione Medio Oriente (EAU)

Medio Oriente (Emirati Arabi Uniti)

- account-part-of-organizations
- acm-certificate-expiration-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- codebuild-project-envvar-awscred-check
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- efs-mount-target-accessibile al pubblico
- eks-cluster-log-enabled

- eks-cluster-secrets-criptato
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- guardduty-s3 abilitato alla protezione

- sono abilitato all'analizzatore di accesso esterno
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-rabbit-deployment-mode
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled

- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

Regione Sud America (San Paolo)

Sud America (San Paolo)

- access-keys-rotated
- account-part-of-organizations

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- crittografia dax-tls-endpoint
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check

- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az

- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-abilitato all'audit di protezione
- abilitato a guardduty-eks-protection-runtime
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty
- guardduty-abilitato alla protezione da malware
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-rds
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- sono abilitato all'analizzatore di accesso esterno

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan abilitato
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check

- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- abilitato per mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-rest
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted

- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled

- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

AWS GovCloud Regione (Stati Uniti orientali)

AWS GovCloud (Stati Uniti orientali)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-last-backup-recovery-point-created
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione
- abilitato a dms-redis-tls
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-user-for-host-mode-check

- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created

- fsx-resources-protected-by-backup-plan
- guardduty-eks-abilitato all'audit di protezione
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- abilitato a inspector-ec2-scan
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- abilitato per mq-cloudwatch-audit-log
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- catalogo di servizi condiviso all'interno dell'organizzazione
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-

- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

AWS GovCloud Regione (Stati Uniti occidentali)

AWS GovCloud (Stati Uniti occidentali)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-last-backup-recovery-point-created
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check

- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- registrazione degli accessi a cloudtrail-s3-bucket
- cloudtrail-s3-bucket-accesso pubblico vietato
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- autenticazione dms-mongo-db abilitata
- dms-neptune-sono abilitato all'autorizzazione

- abilitato a dms-redis-tls
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-accessibile al pubblico
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-secrets-criptato
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-resources-protected-by-backup-plan
- guardduty-eks-abilitato all'audit di protezione
- guardduty-enabled-centralized
- abilitato alla protezione lambda guardduty-lambda
- guardduty-non-archived-findings
- abilitato alla protezione guardduty-s3
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check

- controllo della scadenza del certificato iam-server
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- abilitato a inspector-ec2-scan
- abilitato a inspector-ecr-scan
- inspector-lambda-standard-scan-abilitato
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream crittografato
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- abilitato per mq-cloudwatch-audit-log
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - accesso illimitato alle porte
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited

- abilitato per la replica su più regioni con s3-bucket
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- catalogo di servizi condiviso all'interno dell'organizzazione

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- controllo di restrizione delle porte vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

Regole collegate ai servizi AWS Config

Una AWS Config regola collegata ai servizi è un tipo unico di regole AWS Config gestite che supporta altri AWS servizi per creare AWS Config regole nell'account. Le regole collegate ai servizi sono predefinite e includono tutte le autorizzazioni necessarie per chiamare altri servizi per conto dell'utente. AWS Queste regole sono simili agli standard consigliati da un AWS servizio per la Account AWS verifica della conformità.

Queste AWS Config regole legate ai servizi sono di proprietà dei team di AWS assistenza. Il team AWS di assistenza crea queste regole nel tuo. Account AWS Hai accesso in sola lettura a queste regole. Non puoi modificare o eliminare queste regole se sei abbonato al AWS servizio a cui sono collegate queste regole.

Regole collegate ai servizi e AWS Command Line Interface

Con le AWS CLI API PutConfigRule, DeleteConfig Rule e DeleteEvaluationResults restituiscono l'accesso negato con il seguente messaggio di errore:

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

Regole collegate ai servizi e console AWS Config

Nella AWS Config console, le AWS Config regole collegate al servizio sono visibili nella pagina Regole. I pulsanti Modifica ed Elimina risultati sono di colore grigio nella console per impedire all'utente di modificare la regola. È possibile visualizzare i dettagli della regola selezionando la regola stessa.

Regole collegate ai servizi, azioni correttive e pacchetti di conformità

Per aggiungere azioni di riparazione a regole collegate ai servizi in un pacchetto di conformità, è necessario aggiungere l'azione di correzione al modello di conformità stesso e quindi aggiornare il pacchetto di conformità con il modello aggiornato. Per informazioni sull'aggiornamento dei conformance pack, vedere Distribuzione di un Conformance Pack (console), Distribuzione di un Conformance Pack () e Gestione dei Conformance Pack organizzativi.AWS CLI

Modifica ed eliminazione delle regole collegate ai servizi

Per modificare o eliminare una regola collegata al servizio, contatta il AWS servizio che ha creato la regola. Ad esempio, per le regole collegate ai servizi create da AWS Security Hub, è possibile rimuovere una regola collegata al servizio seguendo questi passaggi nella Guida per l'AWS Security Hub utente: Disabilitazione di uno standard di sicurezza.

Creazione di regole gestite di AWS Config con modelli AWS CloudFormation

> **Important**
>
> È necessario innanzitutto creare e avviare il registratore diAWS Config configurazione per creare regoleAWS Config gestite conAWS CloudFormation. Per ulteriori informazioni, vedere Gestione del registratore di configurazione.

Per le regole gestite di AWS Config che sono supportate, puoi utilizzare i modelli AWS CloudFormation per creare la regola per il tuo account o aggiornare uno stack di AWS CloudFormation esistente. Uno stack è una raccolta di risorse correlate per le quali esegui il

provisioning e l'aggiornamento come unità singola. Quando avvii uno stack con un modello, la regola gestita di AWS Config viene creata per te. I modelli creano solo la regola. Non producono risorse AWS aggiuntive.

> **Note**
>
> Quando le regole gestite di AWS Config vengono aggiornate, anche i modelli sono aggiornati con le modifiche più recenti. Per salvare una versione specifica di un modello per una regola, scarica il modello e caricalo sul tuo bucket S3.

Per ulteriori informazioni sull'utilizzo deiAWS CloudFormation modelli, consulta Guida introduttivaAWS CloudFormation nella Guida per l'AWS CloudFormationutente.

Per avviare uno stack di AWS CloudFormation per una regola gestita di AWS Config

1. Vai alla CloudFormationconsole e crea un nuovo stack.
2. Per Specify template (Specifica modello):
   - Se è stato scaricato il modello, selezionare Upload a template file (Carica un file modello) e scegliere Browse (Sfoglia) per caricare il modello.
   - Puoi anche scegliere l'URL di Amazon S3 e inserire l'URL del modello`http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/`*`THE_RULE_IDENTIFIER`*`.template`.

   > **Note**
   >
   > L'identificatore della regola deve essere scritto in ALL_CAPS_WITH_UNDERSCORES. Ad esempio, CLOUDWATCH_LOG_GROUP_ENCRYPTED anzichécloudwatch-log-group-encrypted.
   > Per alcune regole, l'identificatore della regola è diverso dal nome della regola. Assicurarsi di utilizzare l'identificativo. Ad esempio, l'identificatore della regola per restricted-ssh è INCOMING_SSH_DISABLED.
3. Seleziona Successivo.
4. In Specify stack details (Specifica dettagli stack) digitare il nome di uno stack e immettere i valori dei parametri per la regola AWS Config. Ad esempio, quando utilizzi il modello per la

regola gestita `DESIRED_INSTANCE_TYPE`, puoi specificare il tipo di istanza, come ad esempio "m4.large".

5. Seleziona Successivo.
6. In Options (Opzioni), è possibile creare tag o configurare altre opzioni avanzate. Queste opzioni non sono obbligatorie.
7. Seleziona Successivo.
8. In Review (Revisione), verifica che i parametri del modello e le altre opzioni siano corretti.
9. Seleziona Create (Crea). Lo stack viene creato in pochi minuti. Puoi visualizzare la regola creata nella console di AWS Config.

Puoi utilizzare i modelli per creare un singolo stack per le regole gestite di AWS Config oppure puoi aggiornare uno stack già esistente nell'account. Se elimini uno stack, verranno rimosse anche le regole gestite create da esso. Per ulteriori informazioni, vedere Working with Stacks nella Guida per l'AWS CloudFormationutente.

AWS Config Regole personalizzate

AWS Config Le regole personalizzate sono regole che puoi creare da zero. Esistono due modi per creare regole AWS Config personalizzate: con le funzioni Lambda (AWS Lambda Developer Guide) e con Guard (Guard GitHub Repository), un linguaggio. policy-as-code

AWS Config le regole personalizzate create con Lambda sono chiamate Regole AWS Config Lambda AWS Config personalizzate e le regole personalizzate create con Guard sono chiamate AWS Config Regole di policy personalizzate.

AWS Config Regole di policy personalizzate

Le regole scritte utilizzando Guard possono essere create dalla AWS Config console o utilizzando le API delle AWS Config regole. AWS Config Le regole Custom Policy consentono di creare regole AWS Config personalizzate senza dover utilizzare Java o Python per sviluppare funzioni Lambda per gestire le regole personalizzate. AWS Config Le regole Custom Policy vengono avviate mediante modifiche alla configurazione. Per ulteriori informazioni su Guard, consulta il Guard GitHub Repository.

AWS Config Regole Lambda personalizzate

Le regole Lambda personalizzate offrono la possibilità di utilizzare Java o Python per creare una funzione Lambda per una regola personalizzata. AWS Config Una funzione Lambda è codice personalizzato su cui si carica e viene richiamata da eventi pubblicati su di essa da un'origine di eventi. AWS Lambda Se la funzione Lambda è associata a una AWS Config regola, la AWS Config richiama all'avvio della regola. La funzione Lambda valuta quindi le informazioni di configurazione inviate da e restituisce AWS Config i risultati della valutazione. Per ulteriori informazioni sulle funzioni Lambda, consulta Origini di eventi e funzioni nella Guida per gli sviluppatori di AWS Lambda .

Considerazioni sui costi

Per i dettagli sui costi associati alla registrazione delle risorse, consulta AWS Config i prezzi.

Consiglio: aggiungi la logica per gestire la valutazione delle risorse eliminate per le regole lambda personalizzate

Quando si creano regole lambda AWS Config personalizzate, si consiglia vivamente di aggiungere la logica per gestire la valutazione delle risorse eliminate.

Quando i risultati della valutazione sono contrassegnati come `NOT_APPLICABLE`, verranno contrassegnati per l'eliminazione e ripuliti. Se NON sono contrassegnati come `NOT_APPLICABLE`, i risultati della valutazione rimarranno invariati fino all'eliminazione della regola, il che può causare un picco imprevisto nella creazione di elementi di configurazione per `AWS::Config::ResourceCompliance` al momento dell'eliminazione della regola.

Per informazioni su come impostare regole lambda AWS Config personalizzate da restituire `NOT_APPLICABLE` per le risorse eliminate, consulta Gestione delle risorse eliminate con regole lambda AWS Config personalizzate.

Raccomandazione: fornisci le risorse previste per le regole lambda personalizzate

AWS Config Le regole Lambda personalizzate possono causare un numero elevato di chiamate di funzioni Lambda se la regola non è limitata a uno o più tipi di risorse. Per evitare un aumento dell'attività associata al tuo account, ti consigliamo vivamente di fornire risorse nell'ambito delle regole Lambda personalizzate. Se non viene selezionato alcun tipo di risorsa, la regola richiamerà la funzione Lambda per tutte le risorse dell'account.

Consiglio: interrompi la registrazione della conformità delle risorse prima di eliminare le regole

Si consiglia vivamente di interrompere la registrazione per il tipo di `AWS::Config::ResourceCompliance` risorsa prima di eliminare le regole nell'account. L'eliminazione delle regole crea CI `AWS::Config::ResourceCompliance` e può influire sui costi del registratore AWS Config di configurazione. Se si eliminano regole che valutano un gran numero di tipi di risorse, ciò può portare a un picco nel numero di CI registrati.

Procedura ottimale:

1. Interrompi la registrazione `AWS::Config::ResourceCompliance`
2. Eliminare regole
3. Attiva la registrazione per `AWS::Config::ResourceCompliance`

Tipi di trigger

Dopo aver aggiunto una regola al tuo account, AWS Config confronta le tue risorse con le condizioni della regola. Dopo questa valutazione iniziale, AWS Config continua a eseguire le valutazioni ogni volta che ne viene attivata una. I trigger di valutazione sono definiti come parte della regola e possono includere i seguenti tipi.

Tipo di trigger	Descrizione
Modifiche di configurazione	AWS Config esegue le valutazioni della regola quando esiste una risorsa che corrisponde all'ambito della regola e c'è una modifica nella configurazione della risorsa. La valutazione viene eseguita dopo l' AWS Config invio di una notifica di modifica dell'elemento di configura zione. Puoi scegliere le risorse che avviano la valutazione definendo l'ambito della regola. L'ambito può includere quanto segue: • Uno o più tipi di risorse • Una combinazione di un tipo di risorsa e un ID risorsa

Tipo di trigger	Descrizione
	• Una combinazione di una chiave e un valore di un tag • Quando viene creata, aggiornata o eliminata qualsiasi risorsa registrata AWS Config esegue la valutazione quando rileva una modifica a una risorsa che corrispon de all'ambito della regola. Puoi utilizzare l'ambito per definire le risorse che avviano le valutazioni.
Periodic (Periodico)	AWS Config esegue le valutazioni della regola con una frequenza scelta dall'utente, ad esempio ogni 24 ore.
Ibrido	Alcune regole prevedono sia trigger legati alle modifiche alla configurazione che trigger periodici. Per queste regole, AWS Config valuta le risorse quando rileva una modifica della configurazione e anche alla frequenza specifica ta dall'utente.

Modalità di valutazione

Esistono due modalità di valutazione delle AWS Config regole.

Modalità di valutazione	Descrizione
Proattiva	Utilizza la valutazione proattiva per valutare le risorse prima che vengano implementate. Ciò consente di valutare se un insieme di proprietà della risorsa, se utilizzato per definire una AWS risorsa, sarebbe CONFORME o NON CONFORME, in base all'insieme di regole

Modalità di valutazione	Descrizione
	proattive che hai nel tuo account nella tua regione. Per ulteriori informazioni, consulta Modalità di valutazione. Per un elenco di regole gestite che supportano la valutazione proattiva, vedi Elenco delle regole gestite per modalità di valutazione. AWS Config
Test	Utilizza la valutazione di test per valutare le risorse che sono già state implementate. Ciò consente di valutare le impostazioni di configurazione delle risorse esistenti.

> **Note**
>
> Le regole proattive non correggono le risorse contrassegnate come NON_COMPLIANT e non ne impediscono l'implementazione.

Gestione delle risorse eliminate con regole lambda AWS Config personalizzate

Le regole che segnalano le risorse eliminate devono restituire il risultato della valutazione di `NOT_APPLICABLE` per evitare valutazioni non necessarie delle regole.

Quando elimini una risorsa, AWS Config crea un `configurationItem` con `ResourceDeleted` per. `configurationItemStatus` Puoi utilizzare questi metadati per verificare se una regola segnala una risorsa eliminata. Per ulteriori informazioni sugli elementi di configurazione, consulta Concetti | Elementi di configurazione.

Includi i seguenti frammenti di codice per verificare la presenza di risorse eliminate e imposta il risultato della valutazione di una regola lambda AWS Config personalizzata su `NOT_APPLICABLE` se riporta una risorsa eliminata:

Custom Lambda Rules (Node.js)

```
// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}
```

Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

> **Note**
>
> AWS Config le regole gestite e le regole di policy AWS Config personalizzate gestiscono questo comportamento per impostazione predefinita.
> Se crei una regola lambd AWS Config personalizzata con Python utilizzando AWS Config Development Kit (RDK) AWS Config e Development Kit Library (RdkLib), la classe Evaluator importata controllerà questo comportamento. Per informazioni su come scrivere regole con l'RDK e la RDKlib, consulta Scrittura delle regole con l'RDK e la RDKlib.

Argomenti

- Creazione di regole di policy AWS Config personalizzate
- CreazioneAWS ConfigRegole Lambda personalizzate

Creazione di regole di policy AWS Config personalizzate

Puoi creare regole di policy AWS Config personalizzate da AWS Management Console AWS CLI, o AWS Config API. Per ulteriori informazioni su come scrivere regole con Guard, consulta Writing Guard rules nella AWS CloudFormation Guard User Guide. Per ulteriori informazioni sugli schemi dei tipi di risorse supportati che è AWS Config possibile valutare, vedere resource-types nel Resource Schema Repository. AWS Config GitHub

> **Important**
>
> Lo schema AWS Config delle risorse per valutare gli elementi di configurazione è diverso dallo schema CFN per valutare i modelli. AWS CloudFormation Se utilizzi lo schema CFN per le regole di policy AWS Config personalizzate, i risultati della valutazione restituiranno `NOT_APPLICABLE`. Utilizza lo schema AWS Config delle risorse per creare regole di policy AWS Config personalizzate e scrivi politiche in base alla struttura degli elementi di configurazione. Per un elenco degli schemi di AWS Config risorse, consulta resource-types nel Resource Schema Repository. AWS Config GitHub

Creazione di regole di policy personalizzate AWS Config (Console)

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Nel AWS Management Console menu, verifica che il selettore della regione sia impostato su una AWS regione che supporta AWS Config le regole. Per un elenco delle regioni supportate, consulta Regioni ed endpoint AWS Config in Riferimenti generali di Amazon Web Services.
3. Nel riquadro di navigazione di sinistra seleziona Rules (Regole).
4. Nella pagina Rules (Regole) scegli Add rule (Aggiungi regola).
5. Nella pagina Specifica il tipo di regola, scegli Crea una regola personalizzata utilizzando Guard.
6. Nella pagina Configura regola, crea la regola con la seguente procedura:
   a. In Nome regola, digita un nome univoco per la regola.
   b. In Descrizione, digita una descrizione per la regola.

c. Per la versione runtime di Guard, scegli il sistema di runtime per la tua regola AWS Config Custom Policy.

d. In Contenuti delle regole, puoi inserire la policy Guard personalizzata per la regola. Per ulteriori informazioni sulla struttura e le funzionalità delle politiche di Guard Custom, consulta le modalità operative di AWS CloudFormation Guard 2.0 nel Guard GitHub Repository.

> **Note**
>
> Lo schema AWS Config delle risorse per valutare gli elementi di configurazione è diverso dallo schema CFN per valutare AWS CloudFormation i modelli. Se utilizzi lo schema CFN per le regole di policy AWS Config personalizzate, i risultati della valutazione restituiranno `NOT_APPLICABLE`. Utilizza lo schema AWS Config delle risorse per creare regole di policy AWS Config personalizzate e scrivi politiche in base alla struttura degli elementi di configurazione. Per un elenco degli schemi di AWS Config risorse, consulta resource-types nel Resource Schema Repository. AWS Config GitHub

L'esempio seguente mostra la definizione della politica per una versione della regola AWS Config Custom Policy della Managed rule AWS Config dynamodb-pitr-enabled

```
# This rule checks if point in time recovery (PITR) is enabled on active Amazon
 DynamoDB tables
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
        let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription
        %pitr == "ENABLED"
}
```

e. Per la modalità Valutazione, scegli in che momento del processo di creazione e gestione delle risorse desideri AWS Config valutare le tue risorse. A seconda della regola, è AWS Config possibile valutare le configurazioni delle risorse prima che venga assegnato il provisioning di una risorsa, dopo l'assegnazione di una risorsa o entrambe le cose.

   i. Scegli Attivazione della valutazione proattiva per eseguire valutazioni sulle impostazioni di configurazione delle risorse prima che vengano implementate.

      Dopo aver attivato la valutazione proattiva, puoi utilizzare l'API di StartResourcevalutazione e l'GetResourceEvaluationSummaryAPI per verificare se le risorse specificate in questi comandi verranno contrassegnate come NON_COMPLIANT dalle regole proattive del tuo account nella tua regione.

      Per ulteriori informazioni sull'utilizzo di questi comandi, consulta Evaluating Your Resources with Rules. AWS Config Per un elenco delle regole gestite che supportano la valutazione proattiva, vedere Elenco delle regole AWS Config gestite per modalità di valutazione.

   ii. Seleziona Attivazione della valutazione dei test per valutare le impostazioni di configurazione delle risorse esistenti.

      Per una valutazione approfondita, le regole AWS Config Custom Policy vengono avviate mediante modifiche alla configurazione. Questa opzione sarà preselezionata.

      - Risorse: quando viene creata, modificata o eliminata una risorsa che corrisponde al tipo o al tipo più identificatore specificato.
      - Tag: quando viene creata, modificata o eliminata una risorsa con il tag specificato.
      - Tutte le modifiche: quando una risorsa registrata da AWS Config viene creata, modificata o eliminata.

      AWS Config esegue la valutazione quando rileva una modifica a una risorsa che corrisponde all'ambito della regola. Puoi utilizzare l'ambito per vincolare quali risorse avviano le valutazioni. Altrimenti, le valutazioni vengono avviate quando viene apportata una modifica a una risorsa dopo il suo provisioning.

f. Se la regola include parametri, puoi personalizzare i valori delle chiavi fornite in Parametri. Un parametro è un attributo a cui le risorse devono aderire per essere considerate conformi alla regola.

7. Nella pagina Rivedi e crea, esamina tutte le tue selezioni prima di aggiungere la regola alla tua. Account AWS
8. Al termine della revisione delle regole, scegli Aggiungi regola.

Creazione di regole politiche AWS Config personalizzate ()AWS CLI

Utilizza il comando `put-config-rule`.

Il campo `Owner` deve essere `CUSTOM_POLICY`. I seguenti campi aggiuntivi sono obbligatori per le regole di AWS Config Custom Policy:

- `Runtime`: Il sistema di runtime per le regole AWS Config Custom Policy.
- `PolicyText`: la definizione della policy contenente la logica per le regole di policy AWS Config personalizzate.
- `EnableDebugLogDelivery`: L'espressione booleana per abilitare la registrazione di debug per la regola Custom Policy. AWS Config Il valore predefinito è `false`.

Creazione di regole di policy AWS Config personalizzate (API)

Usa l'azione PutConfigRegola.

Il campo `Owner` deve essere `CUSTOM_POLICY`. I seguenti campi aggiuntivi sono obbligatori per le regole di politica AWS Config personalizzata:

- `Runtime`: Il sistema di runtime per le regole AWS Config Custom Policy.
- `PolicyText`: la policy che definisce la logica per le regole di policy AWS Config personalizzate.
- `EnableDebugLogDelivery`: L'espressione booleana per abilitare la registrazione di debug per la regola Custom Policy. AWS Config Il valore predefinito è `false`.

CreazioneAWS ConfigRegole Lambda personalizzate

Puoi sviluppare regole personalizzate e aggiungerle aAWS ConfigconAWS Lambdafunzioni Associate ogni regola personalizzata a una funzione Lambda, che contiene la logica che valuta seAWSle risorse sono conformi alla regola. Puoi associare questa funzione alla tua regola e la regola richiama la funzione in risposta a modifiche di configurazione oppure periodicamente. La funzione valuta quindi se le risorse sono conformi alla regola e invia i risultati di valutazione a AWS Config.

L'esempio inRegole Lambda personalizzate (esempio di Amazon EC2)ti guida nella creazione di una regola Lambda personalizzata per la prima volta che valuta se ciascuna delle tue istanze EC2 è del tipo t2.micro. Include una funzione Lambda di esempio che puoi aggiungereAWS Lambdasenza alcuna modifica. L'esempio inRegole Lambda personalizzate (esempio generale)fornisce un esempio più generale per la creazione di una regola Lambda personalizzata.

Per scoprire comeAWS Lambdale funzioni funzionano e come svilupparle, vedi ilAWS LambdaGuida per gli sviluppatori.

Argomenti

- Regole Lambda personalizzate (esempio di Amazon EC2)
- Regole Lambda personalizzate (esempio generale)
- Funzioni ed eventi AWS Lambda di esempio per le regole AWS Config

Regole Lambda personalizzate (esempio di Amazon EC2)

Questa procedura ti guida attraverso il processo di creazione di una regola Lambda personalizzata che valuta se ciascuna delle tue istanze EC2 è di tipo t2.micro. AWS Config eseguirà valutazioni basate sugli eventi per questa regola, il che significa che controllerà le configurazioni dell'istanza ogni volta AWS Config che rileva una modifica alla configurazione in un'istanza. AWS Config contrassegnerà le istanze t2.micro come conformi e tutte le altre istanze come non conformi. Lo stato di conformità apparirà nella console AWS Config .

Per ottenere il miglior risultato con questa procedura, dovresti avere una o più istanze EC2 nel tuo. Account AWS Le istanze devono includere una combinazione di almeno una istanza t2.micro e altri tipi.

Per creare questa regola, per prima cosa, creerai una AWS Lambda funzione personalizzando un blueprint nella console. AWS Lambda Quindi, creerai una regola Lambda personalizzata in AWS Config e assocerai la regola alla funzione.

Argomenti

- Creazione di una funzione AWS Lambda per una regola di configurazione personalizzata
- Creazione di una regola Lambda personalizzata per valutare le istanze Amazon EC2

Creazione di una funzione AWS Lambda per una regola di configurazione personalizzata

1. Accedi AWS Management Console e apri la AWS Lambda console all'indirizzo https://console.aws.amazon.com/lambda/.
2. Nel AWS Management Console menu, verifica che il selettore di regione sia impostato su una regione che supporta AWS Config le regole. Per un elenco delle regioni supportate, consultaRegioni ed endpoint di AWS Config nei Riferimenti generali di Amazon Web Services.
3. Nella AWS Lambda console, scegli Crea una funzione Lambda.
4. Scegli Usa uno schema. Nella barra di ricerca, digita config-rule-change-triggered. Seleziona lo schema nei risultati del filtro e scegli Configura.
5. Nella pagina Configure triggers (Configura trigger) scegli Next (Successivo).
6. Nella pagina Informazioni di base, esegui queste operazioni:
   a. Per Function name (Nome funzione), immettere **`InstanceTypeCheck`**.
   b. Per Ruolo di esecuzione, scegli Crea nuovo ruolo dai modelli di AWS policy.
   c. Per Runtime, mantieni Node.js.
   d. In Nome ruolo, digita un nome.
   e. In Modelli di policy, scegli Autorizzazioni regole AWS Config .
   f. Per la funzione di codice della funzione Lambda, mantieni il codice preconfigurato. Il codice Node.js per la tua funzione viene fornito nell'editor di codice. Per questa procedura, non è necessario modificare il codice.
   g. Verifica i dettagli, quindi scegli Crea funzione. La AWS Lambda console mostra la tua funzione.
7. Per verificare che la tua funzione sia configurata correttamente, testala con i seguenti passaggi:
   a. Scegli Test dal menu sotto Panoramica della funzione, quindi scegli Configura evento di test.
   b. In Modello, scegli Notifica della modifica di un elemento di configurazione di AWS Config .
   c. Digitare un nome nel campo Name (Nome).
   d. Scegli Test. AWS Lambda verifica la tua funzione con l'evento di esempio. Se la funzione funziona correttamente, verrà visualizzato un messaggio di errore simile al seguente nella sezione Risultato esecuzione:

```
{
  "errorType": "InvalidResultTokenException,"
  "errorMessage": "Result Token provided is invalid",
```

```
. . .
```

`InvalidResultTokenException`È previsto perché la funzione viene eseguita correttamente solo quando riceve un token di risultato da AWS Config. Il risultato del token identifica la regola AWS Config e l'evento che ha determinato la valutazione e il risultato del token associa una valutazione con una regola. Questa eccezione indica che la funzione dispone dell'autorizzazione necessaria a inviare i risultati a AWS Config. In caso contrario, viene visualizzato il seguente messaggio di errore: `not authorized to perform: config:PutEvaluations`. Se si verifica questo errore, aggiorna il ruolo assegnato alla funzione per consentire l'operazione `config:PutEvaluations` e testare nuovamente la funzione.

Creazione di una regola Lambda personalizzata per valutare le istanze Amazon EC2

1. Apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Nel AWS Management Console menu, verifica che il selettore di regione sia impostato sulla stessa regione in cui hai creato la AWS Lambda funzione per la tua regola Lambda personalizzata.
3. Nella pagina Rules (Regole) scegli Add rule (Aggiungi regola).
4. Nella pagina Specifica il tipo di regola, scegli Crea regola personalizzata.
5. Nella pagina Configure rule (Configura regola) completa la procedura riportata di seguito:
   a. In Name (Nome) digitare **`InstanceTypesAreT2micro`**.
   b. In Description (Descrizione), digitare **`Evaluates whether EC2 instances are the t2.micro type`**.
   c. Per l' ARN della funzione AWS Lambda , specifica l'ARN che AWS Lambda ha assegnato per la funzione.

> **Note**
>
> L'ARN che specifichi in questo passaggio non deve includere il qualificatore `$LATEST`. È possibile specificare un ARN senza un qualificatore di versione o con qualsiasi altro qualificatore. `$LATEST` AWS Lambda supporta il controllo delle versioni delle funzioni e a ciascuna versione viene assegnato un ARN con un

qualificatore. AWS Lambda utilizza il `$LATEST` qualificatore per la versione più recente.

d. In Tipo di trigger, scegli Quando cambia la configurazione.

e. Per Scope of changes (Ambito delle modifiche), scegli Resources (Risorse).

f. In Risorse, scegli Istanza AWS EC2 dall'elenco a discesa Tipo di risorsa.

g. Nella sezione Parametri, è necessario specificare il parametro della regola valutato dalla AWS Lambda funzione e il valore desiderato. La funzione per questa procedura valuta il parametro `desiredInstanceType`.

   In Chiave digitare **`desiredInstanceType`**. In Value (Valore), digita **`t2.micro`**.

6. Seleziona Successivo. Nella pagina Verifica e crea, verifica i dettagli della regola e seleziona Aggiungi funzione regola. La nuova regola viene visualizzata nella pagina Rules (Regole).

   Verrà visualizzato Conformità in corso di valutazione... finché non AWS Config riceve i risultati della valutazione dalla tua AWS Lambda funzione. Se la regola e la funzione funzionano come previsto, viene visualizzato un riepilogo dei risultati dopo alcuni minuti. Ad esempio, il risultato 2 noncompliant resource(s) (2 risorsa/e non conforme/i) indica che 2 non sono istanze t2.micro e il risultato Compliant (Conforme) indica che tutte le istanze sono t2.micro. È possibile aggiornare i risultati con il pulsante di aggiornamento.

   Se la regola o la funzione non funziona correttamente, è possibile visualizzare uno dei risultati seguenti per Compliance (Conformità):

   - Nessun risultato riportato: hai AWS Config valutato le tue risorse rispetto alla regola. L'ambito della regola non si applica alle risorse AWS , le risorse specificate sono state eliminate oppure sono stati eliminati i risultati della valutazione. Per ottenere i risultati della valutazione, aggiorna la regola, modifica l'ambito o seleziona Re-evaluate (Valuta di nuovo).

     Verifica che l'ambito includa Istanza AWS EC2 in Risorse e riprova.

   - Nessuna risorsa inclusa: AWS Config non è possibile valutare le AWS risorse registrate in base a questa regola perché nessuna delle risorse rientra nell'ambito della regola. Per ottenere i risultati della valutazione, modifica la regola e cambiane l'ambito oppure aggiungi risorse da AWS Config registrare utilizzando la pagina Impostazioni.

     Verifica che AWS Config stia registrando le istanze EC2.

- Evaluations failed (Valutazioni non riuscite) Per le informazioni che possono aiutare a determinare il problema, scegli il nome della regola per aprire la relativa pagina dei dettagli e visualizzare il messaggio di errore.

Se la tua regola funziona correttamente e AWS Config fornisce risultati di valutazione, puoi scoprire quali condizioni influiscono sullo stato di conformità della regola. È possibile scoprire quali eventuali risorse non sono conformi e perché. Per ulteriori informazioni, consulta Visualizzazione delle informazioni sulla conformità e dei risultati della valutazione.

Regole Lambda personalizzate (esempio generale)

Completa la procedura seguente per creare una regola Lambda personalizzata. Per creare una regola Lambda personalizzata, devi prima creare una AWS Lambda funzione che contiene la logica di valutazione per la regola. Quindi, associa la funzione a una regola Lambda personalizzata creata in AWS Config.

> **Important**
>
> Come best practice di sicurezza per consentire l' AWS Config autorizzazione a richiamare la funzione Lambda, consigliamo vivamente di limitare l'accesso nella politica basata sulle risorse per `sourceARN` `sourceAccountId` Lambda con e/o nella richiesta di invoca. Per ulteriori informazioni, consulta Best practice di sicurezza per la policy AWS Lambda basata sulle risorse.

Indice

- Creazione di una funzione AWS Lambda per una regola di configurazione personalizzata
- Creazione di una regola personalizzata in AWS Config
- Best practice di sicurezza per la policy AWS Lambda basata sulle risorse
- Valutazione tipi di risorse aggiuntive

Creazione di una funzione AWS Lambda per una regola di configurazione personalizzata

Una funzione Lambda è codice personalizzato su cui si carica e viene richiamata da eventi pubblicati su di essa da un'origine di eventi. AWS Lambda Se la funzione Lambda è associata a una regola Config, la AWS Config richiama quando si verifica l'attivazione della regola. La funzione Lambda

valuta quindi le informazioni di configurazione inviate da AWS Config e restituisce i risultati di valutazione. Per ulteriori informazioni sulle funzioni Lambda, consulta Origini di eventi e funzioni nella Guida per gli sviluppatori di AWS Lambda .

È possibile utilizzare un linguaggio di programmazione supportato da AWS Lambda per creare una funzione Lambda per una regola Lambda personalizzata. Per semplificare questa attività, è possibile personalizzare un AWS Lambda blueprint o riutilizzare una funzione di esempio dal repository Rules. AWS Config GitHub

Piani AWS Lambda

La AWS Lambda console fornisce funzioni di esempio, o blueprint, che è possibile personalizzare aggiungendo la propria logica di valutazione. Quando si crea una funzione, è possibile scegliere uno dei seguenti piani:

- config-rule-change-triggered— Attivato quando le configurazioni AWS delle risorse cambiano.
- config-rule-periodic— Attivato con una frequenza scelta dall'utente (ad esempio, ogni 24 ore).

AWS Config Archivio delle regole GitHub

È disponibile un archivio pubblico di funzioni di esempio per le regole Lambda personalizzate, un servizio GitHub di hosting e condivisione di codice basato sul Web. Le funzioni di esempio sono sviluppate e fornite dalla community. AWS Se si desidera utilizzare un esempio, è possibile copiarne il codice in una nuova AWS Lambda funzione. Per visualizzare il repository, consulta https://github.com/awslabs/aws-config-rules/.

Per creare la funzione per la regola personalizzata

1. Accedi AWS Management Console e apri la AWS Lambda console all'indirizzo https://console.aws.amazon.com/lambda/.
2. Nel AWS Management Console menu, verifica che il selettore di regione sia impostato su una regione che supporta AWS Config le regole. Per un elenco delle regioni supportate, consultaRegioni ed endpoint di AWS Config nei Riferimenti generali di Amazon Web Services.
3. Scegliere Create a Lambda function (Crea una funzione Lambda).
4. Nella pagina Usa un blueprint, puoi scegliere una delle funzioni del blueprint per le AWS Config regole come punto di partenza oppure puoi procedere senza un blueprint scegliendo Ignora.
5. Nella pagina Configure triggers (Configura trigger) scegli Next (Successivo).
6. Nella pagina Informazioni di base, digita un nome e una descrizione.

7. Per Runtime, scegli il linguaggio di programmazione in cui è scritta la funzione.
8. In Code entry type (Tipo di immissione codice), scegli il tipo di voce preferito. Se utilizzi uno schema, mantieni il codice preconfigurato.
9. Fornisci il codice utilizzando il metodo richiesto dal tipo di immissione codice selezionato. Se stai usando un piano, il codice della funzione viene fornito nell'editor di codice ed è possibile personalizzarlo per includere la propria logica di valutazione. Il codice può valutare i dati degli eventi AWS Config forniti quando richiama la funzione:
   - Per le funzioni basate sul config-rule-change-triggeredblueprint o per le funzioni attivate da modifiche alla configurazione, i dati dell'evento sono l'elemento di configurazione o un oggetto di elemento di configurazione sovradimensionato per la risorsa che è stata modificata. AWS
   - Per le funzioni basate sul config-rule-periodicblueprint o per le funzioni attivate con una frequenza scelta dall'utente, i dati dell'evento sono un oggetto JSON che include informazioni su quando è stata attivata la valutazione.
   - Per entrambi i tipi di funzioni, AWS Config passa i parametri delle regole in formato JSON. Puoi definire quali parametri della regola trasmettere quando crei la regola Lambda personalizzata in AWS Config.
   - Ad esempio, gli eventi che vengono AWS Config pubblicati quando richiama la tua funzione, vedi. Esempio eventi per le regole AWS Config
10. In Ruolo di esecuzione, scegli Crea nuovo ruolo dai modelli di policy di AWS .
11. In Role Name (Nome ruolo) digita un nome.
12. In Policy templates (Modelli di policy), scegli AWS Config Rules permission (Autorizzazione regole di configurazione).
13. Verifica i dettagli, quindi scegli Crea funzione.

Creazione di una regola personalizzata in AWS Config

Da utilizzare AWS Config per creare una regola Lambda personalizzata e associarla a una funzione Lambda.

Per creare una regola personalizzata

1. Apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Nel AWS Management Console menu, verifica che il selettore di regione sia impostato sulla stessa regione in cui hai creato la AWS Lambda funzione per la tua regola Lambda personalizzata.

3. Nella pagina Rules (Regole) scegli Add rule (Aggiungi regola).
4. Nella pagina Specifica il tipo di regola, scegli Crea regola personalizzata.
5. Nella pagina Configure rule (Configura regola) digita un nome e la descrizione.
6. Per l' ARN della funzione AWS Lambda , specifica l'ARN che AWS Lambda ha assegnato per la funzione.

> **Note**
>
> L'ARN che specifichi in questo passaggio non deve includere il qualificatore `$LATEST`. È possibile specificare un ARN senza un qualificatore di versione o con qualsiasi altro qualificatore. `$LATEST` AWS Lambda supporta il controllo delle versioni delle funzioni e a ciascuna versione viene assegnato un ARN con un qualificatore. AWS Lambda utilizza il `$LATEST` qualificatore per la versione più recente.

7. Per Trigger type (Tipo di trigger) scegli una o entrambe le opzioni seguenti:
   - Modifiche alla configurazione: AWS Config richiama la funzione Lambda quando rileva una modifica alla configurazione.
   - Periodico: AWS Config richiama la funzione Lambda alla frequenza scelta (ad esempio, ogni 24 ore).
8. Se i tipi di trigger per la tua regola includono modifiche alla configurazione, specifica una delle seguenti opzioni per Ambito delle modifiche con cui AWS Config richiama la tua funzione Lambda:
   - Tutte le modifiche: quando una risorsa registrata da AWS Config viene creata, modificata o eliminata.
   - Risorse: quando viene creata, modificata o eliminata una risorsa che corrisponde al tipo o al tipo più identificatore specificato.
   - Tag: quando viene creata, modificata o eliminata una risorsa con il tag specificato
9. Se i tipi di trigger per la tua regola includono Periodic, specifica la Frequenza con cui AWS Config richiama la funzione Lambda.
10. Nella sezione Parametri, specifica tutti i parametri della regola valutati dalla AWS Lambda funzione e il valore desiderato.
11. Seleziona Successivo. Nella pagina Verifica e crea, verifica i dettagli della regola e seleziona Aggiungi funzione regola. La nuova regola viene visualizzata nella pagina Regole.

Verrà visualizzato Conformità in corso di valutazione... fino a quando non AWS Config riceve i risultati della valutazione dalla tua AWS Lambda funzione. Se la regola e la funzione funzionano come previsto, viene visualizzato un riepilogo dei risultati dopo alcuni minuti. È possibile aggiornare i risultati con il pulsante di aggiornamento.

Se la regola o la funzione non funziona correttamente, è possibile visualizzare uno dei risultati seguenti per Compliance (Conformità):

- Nessun risultato riportato: hai AWS Config valutato le tue risorse rispetto alla regola. L'ambito della regola non si applica alle risorse AWS , le risorse specificate sono state eliminate oppure sono stati eliminati i risultati della valutazione. Per ottenere i risultati della valutazione, aggiorna la regola, modifica l'ambito o seleziona Re-evaluate (Valuta di nuovo).

  Questo messaggio potrebbe essere visualizzato anche nel caso in cui non vengano segnalati risultati di valutazione per la regola.
- Nessuna risorsa inclusa: AWS Config non è possibile valutare le AWS risorse registrate in base a questa regola perché nessuna delle risorse rientra nell'ambito della regola. Puoi scegliere quali risorse AWS Config registra nella pagina Settings (Impostazioni).
- Evaluations failed (Valutazioni non riuscite) Per le informazioni che possono aiutare a determinare il problema, scegli il nome della regola per aprire la relativa pagina dei dettagli e visualizzare il messaggio di errore.

> **Note**
>
> Quando crei una regola Lambda personalizzata con la AWS Config console, vengono create automaticamente le autorizzazioni appropriate. Se crei una regola Lambda personalizzata con AWS CLI, devi dare il AWS Config permesso di richiamare la funzione Lambda utilizzando il comando. `aws lambda add-permission` Per ulteriori informazioni, consulta Using Resource-Based Policies for (AWS Lambda Lambda Function Policies) nella Developer Guide.AWS Lambda
> Prima di concedere AWS Config il permesso di richiamare la funzione Lambda, consulta la sezione seguente. Best practice di sicurezza per la policy AWS Lambda basata sulle risorse

Best practice di sicurezza per la policy AWS Lambda basata sulle risorse

Come best practice di sicurezza, per evitare di concedere l'autorizzazione di richiamata all'intero nome del principale del servizio (SPN) per chiamare la funzione Lambda, è fortemente consigliato limitare l'accesso nella policy Lambda basata sulle risorse inserendo `sourceARN` e/o `sourceAccountId` nella richiesta di richiamata.

`sourceARN`È l'ARN della AWS Config regola che richiama la funzione Lambda.

`sourceAccountId` è l'ID dell'account dell'utente che ha creato la regola.

La limitazione dell'accesso nella policy basata sulle risorse di Lambda aiuta a garantire che l'accesso alle risorse AWS Lambda avvenga solo per conto degli utenti e degli scenari previsti.

Per aggiungere l'autorizzazione basata sull'SPN, è necessario utilizzare la seguente interfaccia a riga di comando

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com
```

Per aggiungere autorizzazioni basate SourceAccountId

Prima di creare la regola, puoi aggiungere l'autorizzazione basata su `sourceAccountId` alla policy basata sulle risorse con la seguente interfaccia a riga di comando

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com --source-
account your account ID
```

Per aggiungere entrambe le autorizzazioni SourceArn e quelle SourceAccountId basate

Dopo aver creato la regola, puoi aggiungere l'autorizzazione basata su `sourceARN` alla policy basata sulle risorse con la seguente interfaccia a riga di comando. Ciò consente solo a un ARN specifico della regola di richiamare la funzione Lambda.

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com --source-
account your account ID --source-arn ARN of the created config rule
```

Valutazione tipi di risorse aggiuntive

È possibile creare regole Lambda personalizzate per eseguire valutazioni per tipi di risorse non ancora registrati da. AWS Config Ciò è utile se desideri valutare la conformità di altri tipi di risorse che attualmente AWS Config non vengono registrati. Per un elenco degli ulteriori tipi di risorse che è possibile valutare con le regole Lambda personalizzate, consulta Informazioni di riferimento dei tipi di risorse AWS.

> **Note**
>
> Quando si crea una Lambda personalizzata per un tipo di risorsa non registrato da AWS Config, la regola deve avere il tipo di trigger periodico. Il tipo di trigger per le modifiche alla configurazione non è supportato. Per ulteriori informazioni, consulta Modalità di valutazione e tipi di trigger per AWS Config le regole.

Esempio

1. Desideri valutare i vault Amazon S3 Glacier nell'account. Le risorse del vault Amazon S3 Glacier non sono attualmente registrate da AWS Config.
2. Crei una AWS Lambda funzione che valuta se i tuoi vault di Amazon S3 Glacier soddisfano i requisiti del tuo account.
3. Crei una regola Lambda personalizzata denominata evaluate-glacier-vaultse quindi assegni la tua AWS Lambda funzione alla regola.
4. AWS Config richiama la tua funzione Lambda e quindi valuta i vault di Amazon S3 Glacier rispetto alla tua regola.
5. AWS Config restituisce le valutazioni e puoi visualizzare i risultati di conformità della tua regola.

> **Note**
>
> È possibile visualizzare i dettagli di configurazione nella AWS Config sequenza temporale e cercare risorse nella AWS Config console per individuare le risorse che AWS Config supportano. Se hai configurato AWS Config la registrazione di tutti i tipi di risorse, le nuove risorse supportate verranno registrate automaticamente. Per ulteriori informazioni, consulta Tipi di risorsa supportati.

Funzioni ed eventi AWS Lambda di esempio per le regole AWS Config

Ogni regola Lambda personalizzata è associata a un Lambdafunzione, che è un codice personalizzato che contiene la logica di valutazione della regola. Quando si verifica il trigger per una regola di Config (ad esempio, quandoAWS Configrileva una modifica della configurazione),AWS Configrichiama la funzione Lambda della regola pubblicando unevento, che è un oggetto JSON che fornisce i dati di configurazione valutati dalla funzione.

Per ulteriori informazioni sulle funzioni e sugli eventi diAWS Lambda, consultaFonti di funzioni ed eventinelAWS LambdaGuida per gli sviluppatori.

Argomenti

- AWS Lambda Funzioni di esempio per AWS Config le regole (Node.js)
- Funzioni AWS Lambda di esempio per le regole AWS Config (Python)
- Esempio eventi per le regole AWS Config

AWS Lambda Funzioni di esempio per AWS Config le regole (Node.js)

AWS Lambda esegue funzioni in risposta a eventi pubblicati dai AWS servizi. La funzione per una regola Lambda AWS Config personalizzata riceve un evento pubblicato da AWS Config e utilizza quindi i dati che riceve dall'evento e recupera dall' AWS Config API per valutare la conformità della regola. Le operazioni in una funzione per una regola di configurazione variano a seconda che si esegua una valutazione attivata da modifiche di configurazione o attivata periodicamente.

Per informazioni sui modelli comuni all'interno AWS Lambda delle funzioni, consulta Programming Model nella AWS Lambda Developer Guide.

Indice

- Funzione di esempio per le valutazioni attivate dalle modifiche di configurazione
- Funzione di esempio per valutazioni periodiche

Funzione di esempio per le valutazioni attivate dalle modifiche di configurazione

AWS Config invocherà una funzione come nell'esempio seguente quando rileva una modifica alla configurazione per una risorsa che rientra nell'ambito di una regola personalizzata.

Se utilizzi la AWS Config console per creare una regola associata a una funzione come questo esempio, scegli Modifiche alla configurazione come tipo

di trigger. Se utilizzi l' AWS Config API o AWS CLI per creare la regola, imposta l'`MessageType`attributo su `ConfigurationItemChangeNotification` and`OversizedConfigurationItemChangeNotification`. Queste impostazioni consentono di attivare la regola ogni volta che viene AWS Config generato un elemento di configurazione o un elemento di configurazione sovradimensionato a seguito di una modifica delle risorse.

Questo esempio valuta le risorse e verifica che le istanze corrispondano al tipo di risorsa, `AWS::EC2::Instance`. La regola viene attivata quando AWS Config genera un elemento di configurazione o un notifica di un elemento di configurazione di dimensioni eccessive.

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand, PutEvaluationsCommand }
 from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
    return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory API.
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
```

```
        }
    );

}

// Convert the oversized configuration item from the API model to the original
 invocation model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash =
 apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}

// Based on the message type, get the configuration item either from the
 configurationItem object in the invoking event or with the getResourceConfigHistory
 API in the getConfiguration function.
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem) =>
 {
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
        });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
```

```
    }
}

// Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope ===
 false;
}

// In this example, the resource is compliant if it is an instance and its type matches
 the type specified as the desired type.
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration, 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
export const handler = async (event, context) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
```

```
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
            if (compliance === "NON_COMPLIANT") {
                annotation = "This is an annotation describing why the resource is not
 compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                    Annotation: annotation
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                },
            ];
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
    });
};
```

Operazioni della funzione

La funzione esegue le operazioni seguenti in fase di runtime:

1. La funzione viene eseguita quando AWS Lambda passa l'`event`oggetto alla `handler` funzione. In questo esempio, la funzione accetta il `callback` parametro opzionale, che utilizza per restituire

informazioni al chiamante. AWS Lambda passa anche un `context` oggetto, che contiene informazioni e metodi che la funzione può utilizzare durante l'esecuzione. Tieni presente che nelle versioni più recenti di Lambda il contesto non è più utilizzato.

2. La funzione verifica che il `messageType` per l'evento sia un elemento di configurazione o un elemento di configurazione di dimensioni eccessive e quindi restituisce l'elemento di configurazione.
3. Il gestore chiama la funzione `isApplicable` per determinare se la risorsa sia stato eliminata.

> **Note**
>
> Le regole che segnalano le risorse eliminate devono restituire il risultato della valutazione di `NOT_APPLICABLE` per evitare valutazioni non necessarie delle regole.

4. Il gestore chiama la `evaluateChangeNotificationCompliance` funzione e passa gli `ruleParameters` oggetti `configurationItem` and AWS Config pubblicati nell'evento.

   La funzione prima valuta se la risorsa è un'istanza EC2. Se la risorsa non è un'istanza EC2, la funzione restituisce un valore di conformità di `NOT_APPLICABLE`.

   La funzione valuta quindi se l'attributo `instanceType` nell'elemento di configurazione sia pari al valore del parametro `desiredInstanceType`. Se i valori sono uguali, la funzione restituisce `COMPLIANT`. Se i valori non sono uguali, la funzione restituisce `NON_COMPLIANT`.
5. Il gestore si prepara a inviare i risultati della valutazione AWS Config inizializzando l'oggetto. `putEvaluationsRequest` Questo oggetto include il parametro `Evaluations`, che identifica il risultato di conformità, il tipo di risorsa e l'ID della risorsa che è stata valutata. L'`putEvaluationsRequest`oggetto include anche il token dei risultati dell'evento, che identifica la regola e l'evento per. AWS Config
6. Il gestore invia i risultati della valutazione AWS Config passando l'oggetto al `putEvaluations` metodo del `config` client.

Funzione di esempio per valutazioni periodiche

AWS Config invocherà una funzione come nell'esempio seguente per le valutazioni periodiche. Le valutazioni periodiche si verificano con la frequenza che specifichi quando definisci la regola in AWS Config.

Se usi la AWS Config console per creare una regola associata a una funzione come questo esempio, scegli Periodic come tipo di trigger. Se utilizzi l' AWS Config API o AWS CLI per creare la regola, imposta l'`MessageType`attributo `ScheduledNotification` su.

Questo esempio verifica se il numero totale di una risorsa specificata supera il limite massimo impostato.

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand, PutEvaluationsCommand }
 from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Receives the event and context from AWS Lambda.
export const handler = async (event, context, callback) => {
    // Parses the invokingEvent and ruleParameters values, which contain JSON objects
 passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        numberOfResources = 0;

    if (isScheduledNotification(invokingEvent) &&
 hasValidRuleParameters(ruleParameters, callback)) {
        await countResourceTypes(ruleParameters.applicableResourceType, "",
 numberOfResources, async function (err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                const compliance = evaluateCompliance(ruleParameters.maxCount, count);
                var annotation = '';
                if (compliance === "NON_COMPLIANT") {
                    annotation = "Description of why the resource is not compliant.";
                }
                // Initializes the request that contains the evaluation results.
                if (annotation) {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date(),
                            Annotation: annotation
```

```
                        }],
                        ResultToken: event.resultToken
                    };
                } else {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date()
                        }],
                        ResultToken: event.resultToken
                    };
                }

                // Sends the evaluation results to AWS Config.
                try {
                    await configClient.send(new
 PutEvaluationsCommand(putEvaluationsRequest));
                }
                catch (e) {
                    callback(e, null);
                }
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
    // Regular express to verify that applicable resource given is a resource type
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
```

```
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource type.",
 null);
    }
    if (!maxCountIsInt) {
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count, callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
    return count;
}
```

Operazioni della funzione

La funzione esegue le operazioni seguenti in fase di runtime:

1. La funzione viene eseguita quando AWS Lambda passa l'`event`oggetto alla `handler` funzione. In questo esempio, la funzione accetta il `callback` parametro opzionale, che utilizza per restituire informazioni al chiamante. AWS Lambda passa anche un `context` oggetto, che contiene informazioni e metodi che la funzione può utilizzare durante l'esecuzione. Tieni presente che nelle versioni più recenti di Lambda il contesto non è più utilizzato.
2. Per contare le risorse del tipo specificato, il gestore chiama la funzione `countResourceTypes` e trasferisce il parametro `applicableResourceType` che ha ricevuto dall'evento. La funzione `countResourceTypes` chiama il metodo `listDiscoveredResources` del client `config`, che restituisce un elenco di identificatori per le risorse applicabili. La funzione utilizza la lunghezza di questo elenco per determinare il numero di risorse applicabili e restituisce questo conteggio al gestore.
3. Il gestore si prepara a inviare i risultati della valutazione AWS Config inizializzando l'oggetto. `putEvaluationsRequest` Questo oggetto include il `Evaluations` parametro, che identifica il risultato di conformità e Account AWS quello che è stato pubblicato nell'evento. Puoi utilizzare il parametro `Evaluations` per applicare il risultato a qualsiasi tipo di risorsa supportata da AWS Config. L'`putEvaluationsRequest`oggetto include anche il token dei risultati dell'evento, che identifica la regola e l'evento per. AWS Config
4. All'interno dell'oggetto `putEvaluationsRequest`, il gestore chiama la funzione `evaluateCompliance`, Questa funzione verifica se il numero di risorse applicabili supera il massimo assegnato al parametro `maxCount`, che è stato fornito dall'evento. Se il numero di risorse supera il limite massimo, la funzione restituisce `NON_COMPLIANT`. Se il numero di risorse non supera il limite massimo, la funzione restituisce `COMPLIANT`.
5. Il gestore invia i risultati della valutazione AWS Config passando l'oggetto al `putEvaluations` metodo del `config` client.

Funzioni AWS Lambda di esempio per le regole AWS Config (Python)

AWS Lambda esegue funzioni in risposta a eventi pubblicati da servizi AWS. La funzione per una regola Lambda AWS Config personalizzata riceve un evento pubblicato da AWS Config. La funzione usa quindi i dati ricevuti dall'evento e che recupera dall'API di AWS Config per valutare la conformità della regola. Le operazioni in una funzione per una regola di configurazione variano a seconda che si esegua una valutazione attivata da modifiche di configurazione o attivata periodicamente.

Per informazioni sui modelli comuni all'interno delle funzioni AWS Lambda, consulta Modello di programmazione nella Guida per gli sviluppatori di AWS Lambda.

Indice

- Funzione di esempio per le valutazioni attivate dalle modifiche di configurazione
- Funzione di esempio per valutazioni periodiche

Funzione di esempio per le valutazioni attivate dalle modifiche di configurazione

AWS Config richiamerà una funzione, come nell'esempio seguente, quando rileva una modifica di configurazione per una risorsa nell'ambito di una regola personalizzata.

Se usi la console AWS Config per creare una regola che è associata a una funzione, come in questo esempio, scegli Configuration changes (Modifiche di configurazione) come tipo di trigger. Se usi l'API AWS Config o AWS CLI per creare la regola, imposta l'attributo `MessageType` su `ConfigurationItemChangeNotification` e `OversizedConfigurationItemChangeNotification`. Queste impostazioni permettono alla regola di essere attivate ogni volta che AWS Config genera un elemento di configurazione o un elemento di configurazione di dimensioni eccessive come risultato di una modifica delle risorse.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
```

```
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] = json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem
```

```
# Based on the type of message get the configuration item
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'], 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')

# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission to
 assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
```

```
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
```

```
        ],
        ResultToken=event['resultToken'])
```

Operazioni della funzione

La funzione esegue le operazioni seguenti in fase di runtime:

1. La funzione viene eseguita quando AWS Lambda trasmette l'oggetto `event` alla funzione `handler`. In questo esempio, la funzione accetta il parametro `callback` opzionale, che utilizza per restituire le informazioni al chiamante. AWS Lambda trasmette anche un oggetto `context`, che contiene informazioni e metodi che la funzione può utilizzare durante l'esecuzione. Tieni presente che nelle versioni più recenti di Lambda il contesto non è più utilizzato.
2. La funzione verifica che il `messageType` per l'evento sia un elemento di configurazione o un elemento di configurazione di dimensioni eccessive e quindi restituisce l'elemento di configurazione.
3. Il gestore chiama la funzione `isApplicable` per determinare se la risorsa sia stato eliminata.

   > **Note**
   >
   > Le regole che segnalano le risorse eliminate devono restituire il risultato della valutazione di `NOT_APPLICABLE` per evitare valutazioni non necessarie delle regole.

4. Il gestore chiama la funzione `evaluateChangeNotificationCompliance` e trasferisce gli oggetti `configurationItem` e `ruleParameters` AWS Config pubblicati nell'evento.

   La funzione prima valuta se la risorsa è un'istanza EC2. Se la risorsa non è un'istanza EC2, la funzione restituisce un valore di conformità di `NOT_APPLICABLE`.

   La funzione valuta quindi se l'attributo `instanceType` nell'elemento di configurazione sia pari al valore del parametro `desiredInstanceType`. Se i valori sono uguali, la funzione restituisce `COMPLIANT`. Se i valori non sono uguali, la funzione restituisce `NON_COMPLIANT`.
5. Il gestore prepara l'invio dei risultati di valutazione a AWS Config inizializzando l'oggetto `putEvaluationsRequest`. Questo oggetto include il parametro `Evaluations`, che identifica il risultato di conformità, il tipo di risorsa e l'ID della risorsa che è stata valutata. L'oggetto `putEvaluationsRequest` include, inoltre, il risultato del token dall'evento, che identifica la regola e l'evento per AWS Config.
6. Il gestore invia i risultati di valutazione a AWS Config trasferendo l'oggetto al metodo `putEvaluations` del client `config`.

Funzione di esempio per valutazioni periodiche

AWS Config richiamerà una funzione simile al seguente esempio per le valutazioni periodiche. Le valutazioni periodiche si verificano con la frequenza che specifichi quando definisci la regola in AWS Config.

Se usi la console AWS Config per creare una regola che è associata a una funzione, come in questo esempio, scegli Periodic (Periodico) come tipo di trigger. Se usi l'API AWS Config o AWS CLI per creare la regola, imposta l'attributo `MessageType` su `ScheduledNotification`.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
```

```
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission to
 assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value to
 the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled rules.
    Keyword arguments:
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
```

```
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report on
 the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    valid_rule_parameters = evaluate_parameters(rule_parameters)

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
 count_resource_types(valid_rule_parameters['applicableResourceType'], '',
 resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
 resource_type=DEFAULT_RESOURCE_TYPE))
```

```
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
ResultToken=event['resultToken'])
```

Operazioni della funzione

La funzione esegue le operazioni seguenti in fase di runtime:

1. La funzione viene eseguita quando AWS Lambda trasmette l'oggetto `event` alla funzione `handler`. In questo esempio, la funzione accetta il parametro `callback` opzionale, che utilizza per restituire le informazioni al chiamante. AWS Lambda trasmette anche un oggetto `context`, che contiene informazioni e metodi che la funzione può utilizzare durante l'esecuzione. Tieni presente che nelle versioni più recenti di Lambda il contesto non è più utilizzato.
2. Per contare le risorse del tipo specificato, il gestore chiama la funzione `countResourceTypes` e trasferisce il parametro `applicableResourceType` che ha ricevuto dall'evento. La funzione `countResourceTypes` chiama il metodo `listDiscoveredResources` del client `config`, che restituisce un elenco di identificatori per le risorse applicabili. La funzione utilizza la lunghezza di questo elenco per determinare il numero di risorse applicabili e restituisce questo conteggio al gestore.
3. Il gestore prepara l'invio dei risultati di valutazione a AWS Config inizializzando l'oggetto `putEvaluationsRequest`. Questo oggetto include il parametro `Evaluations`, che identifica il risultato di conformità e l'Account AWS che è stato pubblicato nell'evento. Puoi utilizzare il parametro `Evaluations` per applicare il risultato a qualsiasi tipo di risorsa supportata da AWS Config. L'oggetto `putEvaluationsRequest` include, inoltre, il risultato del token dall'evento, che identifica la regola e l'evento per AWS Config.
4. All'interno dell'oggetto `putEvaluationsRequest`, il gestore chiama la funzione `evaluateCompliance`, Questa funzione verifica se il numero di risorse applicabili supera il massimo assegnato al parametro `maxCount`, che è stato fornito dall'evento. Se il numero di risorse supera il limite massimo, la funzione restituisce `NON_COMPLIANT`. Se il numero di risorse non supera il limite massimo, la funzione restituisce `COMPLIANT`.
5. Il gestore invia i risultati di valutazione a AWS Config trasferendo l'oggetto al metodo `putEvaluations` del client `config`.

Esempio eventi per le regole AWS Config

Quando si verifica l'attivazione di una regola, AWS Config richiama la AWS Lambda funzione della regola pubblicando un evento. Quindi AWS Lambda esegue la funzione passando l'evento al gestore della funzione.

Evento di esempio per le valutazioni attivate dalle modifiche di configurazione

AWS Config pubblica un evento quando rileva una modifica alla configurazione per una risorsa che rientra nell'ambito di una regola. L'esempio seguente mostra che la regola è stata attivata da una modifica di configurazione per un'istanza EC2.

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Evento di esempio per le valutazioni attivate dalle modifiche di configurazione di dimensioni eccessive

Alcune modifiche delle risorse generano elementi di configurazione di dimensioni eccessive. L'esempio seguente mostra che la regola è stata attivata da una modifica di configurazione di dimensioni eccessive per un'istanza EC2.

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
```

```
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

Evento di esempio per le valutazioni attivate con frequenza periodica

AWS Config pubblica un evento quando valuta le risorse con una frequenza specificata dall'utente (ad esempio ogni 24 ore). Il seguente evento di esempio mostra che la regola è stata attivata con frequenza periodica.

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime\":
\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",\"recordVersion
\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Attributi di eventi

L'oggetto JSON per un AWS Config evento contiene i seguenti attributi:

`invokingEvent`

L'evento che attiva la valutazione di una regola. Se l'evento viene pubblicato in risposta a una modifica di configurazione delle risorse, il valore per questo attributo è una stringa che contiene un JSON `configurationItem` o un `configurationItemSummary` (per gli elementi di configurazione dimensioni eccessive). L'elemento di configurazione rappresenta lo stato della risorsa nel momento in cui è AWS Config stata rilevata la modifica. Per un esempio di elemento di configurazione, vedete l'output prodotto dal `get-resource-config-history` AWS CLI comando inVisualizzazione della cronologia della configurazione.

Se l'evento viene pubblicato per una valutazione periodica, il valore è una stringa che contiene un oggetto JSON. L'oggetto include informazioni sulla valutazione che è stata attivata.

Per ogni tipo di evento, una funzione deve analizzare la stringa con un parser JSON per poter valutare il contenuto, come illustrato nel seguente esempio Node.js:

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

Coppie chiave-valore che la funzione elabora come parte della sua logica di valutazione. I parametri vengono definiti quando si utilizza la AWS Config console per creare una regola Lambda personalizzata. Puoi anche definire i parametri con l'`InputParameters`attributo nella richiesta `PutConfigRule` AWS Config API o nel `put-config-rule` AWS CLI comando.

Il codice JSON per i parametri è contenuto all'interno di una stringa, perciò una funzione deve analizzare la stringa con un parser JSON per essere in grado di valutare il contenuto, come illustrato nel seguente esempio Node.js:

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

Un token a cui la funzione deve passare AWS Config con la `PutEvaluations` chiamata.

`eventLeftScope`

Un valore booleano che indica se la AWS risorsa da valutare è stata rimossa dall'ambito della regola. Se il valore è `true`, la funzione indica che la valutazione può essere ignorata

passando `NOT_APPLICABLE` come valore per l'attributo `ComplianceType` nella chiamata `PutEvaluations`.

`executionRoleArn`

L'ARN del ruolo IAM a cui è assegnato. AWS Config

`configRuleArn`

L'ARN AWS Config assegnato alla regola.

`configRuleName`

Il nome assegnato alla regola che ha causato AWS Config la pubblicazione dell'evento e il richiamo della funzione.

`configRuleId`

L'ID AWS Config assegnato alla regola.

`accountId`

L'ID del Account AWS proprietario della regola.

`version`

Un numero di versione assegnato da AWS. La versione aumenterà se AWS aggiunge attributi agli AWS Config eventi. Se una funzione richiede un attributo solo in eventi che soddisfano o superano una versione specifica, la funzione può controllare il valore dell'attributo.

La versione attuale per AWS Config gli eventi è la 1.0.

Aggiungere, aggiornare ed eliminare regole AWS Config

Puoi utilizzare la AWS Config console o gli AWS SDK per visualizzare, aggiungere ed eliminare le tue regole.

Aggiunta, visualizzazione, aggiornamento ed eliminazione delle regole (console)

Nella pagina Regole puoi visualizzare una tabella con le regole e i relativi risultati di conformità correnti. Il risultato per ogni regola è Evaluating... fino al AWS Config termine della valutazione delle risorse in base alla regola. È possibile aggiornare i risultati con il pulsante di aggiornamento. Al AWS

Config termine delle valutazioni, è possibile visualizzare le regole e i tipi di risorse conformi o non conformi. Per ulteriori informazioni, consulta Visualizzazione delle informazioni sulla conformità e dei risultati della valutazione.

> **Note**
>
> AWS Config valuta solo i tipi di risorse che sta registrando. Ad esempio, se aggiungi la regola abilitata per cloudtrail ma non registri il tipo di risorsa CloudTrail trail, non AWS Config puoi valutare se i percorsi del tuo account sono conformi o non conformi. Per ulteriori informazioni, consulta AWS Risorse per la registrazione.

Aggiunta di regole

Per aggiungere una regola

1. Accedi e apri la console all'indirizzo https://console.aws.amazon.com/config/. AWS Management ConsoleAWS Config
2. Nel AWS Management Console menu, verifica che il selettore di regione sia impostato su una regione che supporta AWS Config le regole. Per un elenco delle regioni supportate, consultaRegioni ed endpoint di AWS Config nei Riferimenti generali di Amazon Web Services.
3. Nel riquadro di navigazione di sinistra seleziona Rules (Regole).
4. Nella pagina Rules (Regole) scegli Add rule (Aggiungi regola).
5. Nella pagina Specifica il tipo di regola, specifica il tipo di regola completando i seguenti passaggi:
   a. Nel campo di ricerca, indica se filtrare l'elenco delle regole gestite in base al nome, alla descrizione o all'etichetta della regola. Ad esempio, digita EC2 per visualizzare le regole che valutano i tipi di risorse di EC2 oppure digita periodic (periodico) per ottenere le regole con trigger periodici.
   b. Puoi anche creare regole personalizzate. Scegli Crea regola personalizzata usando Lambda o Crea regola personalizzata usando Guard e segui la procedura in Creazione di regole AWS Config Lambda personalizzate o AWS Config Creazione di regole di policy personalizzate.
6. Nella pagina Configura la regola, configura la regola con la seguente procedura:
   a. In Name (Nome), digita un nome univoco per la regola.
   b. In Descrizione, digita una descrizione per la regola.

c. Per la modalità Valutazione, scegli in che momento del processo di creazione e gestione delle risorse desideri AWS Config valutare le tue risorse. A seconda della regola, è AWS Config possibile valutare le configurazioni delle risorse prima che una risorsa venga distribuita, dopo la distribuzione di una risorsa o entrambe le cose.

   i. Scegli Attivazione della valutazione proattiva per eseguire valutazioni sulle impostazioni di configurazione delle risorse prima che vengano implementate.

      Dopo aver attivato la valutazione proattiva, puoi utilizzare l'API di StartResourcevalutazione e l'GetResourceEvaluationSummaryAPI per verificare se le risorse specificate in questi comandi verranno contrassegnate come NON_COMPLIANT dalle regole proattive del tuo account nella tua regione.

      Per ulteriori informazioni sull'utilizzo di questi comandi, consulta Evaluating Your Resources with Rules. AWS Config Per un elenco delle regole gestite che supportano la valutazione proattiva, vedere Elenco delle regole AWS Config gestite per modalità di valutazione.

   ii. Seleziona Attivazione della valutazione dei test per valutare le impostazioni di configurazione delle risorse esistenti.

      Per la valutazione dei test, esistono due tipi di trigger: Quando cambia la configurazione e Periodica.

      A. Se i tipi di trigger per la tua regola includono modifiche alla configurazione, specifica una delle seguenti opzioni per Ambito delle modifiche con cui AWS Config richiama la tua funzione Lambda:

         - Risorse: quando viene creata, modificata o eliminata una risorsa che corrisponde al tipo o al tipo più identificatore specificato.
         - Tag: quando viene creata, modificata o eliminata una risorsa con il tag specificato.
         - Tutte le modifiche: quando una risorsa registrata da AWS Config viene creata, modificata o eliminata.

         AWS Config esegue la valutazione quando rileva una modifica a una risorsa che corrisponde all'ambito della regola. Puoi utilizzare l'ambito per definire le risorse che avviano le valutazioni.

B. Se i tipi di trigger per la tua regola includono Periodic, specifica la Frequenza con cui AWS Config richiama la funzione Lambda.

d. Se la regola include parametri, puoi personalizzare i valori delle chiavi fornite in Parametri. Un parametro è un attributo a cui le risorse devono aderire per essere considerate conformi alla regola.

7. Nella pagina Rivedi e crea, esamina tutte le tue selezioni prima di aggiungere la regola alla tua. Account AWS Se la regola non funziona come previsto, puoi visualizzare uno dei risultati seguenti in Conformità:

   - Nessun risultato riportato: hai AWS Config valutato le tue risorse rispetto alla regola. La regola non si applicava alle AWS risorse incluse nel suo ambito, le risorse specificate sono state eliminate o i risultati della valutazione sono stati eliminati. Per ottenere i risultati della valutazione, aggiorna la regola, modifica l'ambito o seleziona Re-evaluate (Valuta di nuovo).

     Questo messaggio potrebbe essere visualizzato anche nel caso in cui non vengano segnalati risultati di valutazione per la regola.
   - Nessuna risorsa inclusa: AWS Config non è possibile valutare le AWS risorse registrate in base a questa regola perché nessuna delle risorse rientra nell'ambito della regola. Per ottenere i risultati della valutazione, modifica la regola e cambiane l'ambito oppure aggiungi risorse da AWS Config registrare utilizzando la pagina Impostazioni.
   - Evaluations failed (Valutazioni non riuscite) Per le informazioni che possono aiutare a determinare il problema, scegli il nome della regola per aprire la relativa pagina dei dettagli e visualizzare il messaggio di errore.

Visualizzazione delle regole

Per visualizzare le regole

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Nel AWS Management Console menu, verifica che il selettore di regione sia impostato su una regione che supporta AWS Config le regole. Per un elenco delle regioni supportate, consultaRegioni ed endpoint di AWS Config nei Riferimenti generali di Amazon Web Services.
3. Nel riquadro di navigazione di sinistra seleziona Rules (Regole).
4. La pagina Regole mostra tutte le regole attualmente presenti nel tuo Account AWS. Sono riportati il nome, l'azione di riparazione associata e lo stato di conformità di ogni regola.

- Per iniziare la creazione di una regola, seleziona Add rule (Aggiungi regola).
- Scegli una regola per visualizzarne le impostazioni oppure scegli una regola e seleziona Visualizza dettagli.
- Vedi lo stato di conformità della regola quando esegue la valutazione delle risorse.
- Scegli una regola e seleziona Modifica regola per modificare le impostazioni di configurazione della regola e impostare un'azione di riparazione per una regola non conforme.

Aggiornamento delle regole

Per aggiornare una regola

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Nel AWS Management Console menu, verifica che il selettore di regione sia impostato su una regione che supporta AWS Config le regole. Per un elenco delle regioni supportate, consultaRegioni ed endpoint di AWS Config nei Riferimenti generali di Amazon Web Services.
3. Nel riquadro di navigazione di sinistra seleziona Rules (Regole).
4. Scegli una regola e seleziona Modifica regola per la regola da aggiornare.
5. Cambia le impostazioni nella pagina Modifica regola per modificare la regola in base alle esigenze.
6. Selezionare Salva.

Eliminazione delle regole

Per eliminare una regola

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Nel AWS Management Console menu, verifica che il selettore di regione sia impostato su una regione che supporta AWS Config le regole. Per un elenco delle regioni supportate, consultaRegioni ed endpoint di AWS Config nei Riferimenti generali di Amazon Web Services.
3. Nel riquadro di navigazione di sinistra seleziona Rules (Regole).
4. Dalla tabella, scegli una regola da eliminare.
5. Dall'elenco a discesa Azioni, scegli Elimina regola.

6. Quando richiesto, digita "Delete" (questa voce fa distinzione tra maiuscole e minuscole), quindi seleziona Elimina.

Attivazione della valutazione proattiva

Puoi utilizzare la valutazione proattiva per valutare le risorse prima che vengano implementate. Ciò ti consente di valutare se un insieme di proprietà della risorsa, se utilizzato per definire una AWS risorsa, sarebbe CONFORME o NON_COMPLIANT, in base all'insieme di regole proattive che hai nel tuo account nella tua regione.

Lo schema del tipo di risorsa indica le proprietà di una risorsa. Puoi trovare lo schema del tipo di risorsa nelle "estensioni AWS pubbliche" all'interno del AWS CloudFormation registro o con il seguente comando CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Per ulteriori informazioni, consulta Gestione delle estensioni tramite il AWS CloudFormation registro e il riferimento ai tipi di AWS risorse e proprietà nella Guida per l' AWS CloudFormation utente.

> **Note**
>
> Le regole proattive non correggono le risorse contrassegnate come NON_COMPLIANT e non ne impediscono l'implementazione.

Per attivare la valutazione proattiva

1. Accedere AWS Management Console e aprire la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Nel AWS Management Console menu, verifica che il selettore della regione sia impostato su una regione che supporta AWS Config le regole. Per un elenco delle regioni AWS supportate, consulta Regioni ed endpoint AWS Config in Riferimenti generali di Amazon Web Services.
3. Nel riquadro di navigazione di sinistra seleziona Rules (Regole). Per un elenco di regole gestite che supportano la valutazione proattiva, vedi Elenco delle regole AWS Config gestite per modalità di valutazione.
4. Seleziona una regola e scegli Modifica regola per la regola che desideri aggiornare.

5. In Modalità di valutazione, scegli Attivazione della valutazione proattiva per eseguire valutazioni sulle impostazioni di configurazione delle risorse prima che vengano implementate.
6. Selezionare Salva.

Dopo aver attivato la valutazione proattiva, puoi utilizzare l'API di StartResourcevalutazione e l'GetResourceEvaluationSummaryAPI per verificare se le risorse specificate in questi comandi verranno contrassegnate come NON_COMPLIANT dalle regole proattive del tuo account nella tua regione.

Ad esempio, inizia con l'API: StartResourceEvaluation

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Viene visualizzato `ResourceEvaluationId` nell'output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Quindi, utilizza `ResourceEvaluationId` con l' GetResourceEvaluationSummary API per verificare il risultato della valutazione:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Riceverai un output simile al seguente:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
```

```
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Per visualizzare informazioni aggiuntive sul risultato della valutazione, ad esempio la regola che ha contrassegnato una risorsa come NON_COMPLIANT, utilizza l'API Resource. GetCompliance DetailsBy

Visualizza, aggiorna o aggiungi ed elimina regole (SDK)AWS

Visualizzazione delle regole

I seguenti esempi di codice mostrano come utilizzare`DescribeConfigRules`.

CLI

AWS CLI

Per ottenere i dettagli di una regola di AWS Config

Il comando seguente restituisce i dettagli per una regola AWS Config denominata: `InstanceTypesAreT2micro`

```
aws configservice describe-config-rules --config-rule-names
 InstanceTypesAreT2micro
```

Output:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
```

```
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- Per i dettagli sull'API, consulta DescribeConfigRules in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio elenca le regole di configurazione per l'account, con le proprietà selezionate.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Output:

```
ConfigRuleName                                      ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                      ------------
 -------------
 ---------------
```

```
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Per i dettagli sull'API, vedere DescribeConfigRules in AWS Tools for PowerShell Cmdlet Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
```

```
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- Per i dettagli sull'API, consulta DescribeConfigRules in AWS SDK for Python (Boto3) API Reference.

Aggiornamento o aggiunta di regole

I seguenti esempi di codice mostrano come utilizzare. `PutConfigRule`

CLI

AWS CLI

Per aggiungere una regola AWS Config gestita

Il comando seguente fornisce codice JSON per aggiungere una regola Config AWS gestita:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json`è un file JSON che contiene la configurazione delle regole:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
```

```
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Per l'`ComplianceResourceTypes`attributo, questo codice JSON limita l'ambito alle risorse del `AWS::EC2::Instance` tipo, quindi AWS Config valuterà solo le istanze EC2 rispetto alla regola. Poiché la regola è una regola gestita, l'`Owner`attributo è impostato su e l'`SourceIdentifier`attributo è impostato sull'identificatore della regola`AWS`,. `REQUIRED_TAGS` Per l'`InputParameters`attributo, vengono specificate le chiavi di tag richieste dalla regola `CostCenter` e`Owner`.

Se il comando ha esito positivo, AWS Config non restituisce alcun output. Per verificare la configurazione della regola, esegui il describe-config-rules comando e specifica il nome della regola.

Per aggiungere una regola Config gestita dal cliente

Il comando seguente fornisce il codice JSON per aggiungere una regola Config gestita dal cliente:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json`è un file JSON che contiene la configurazione delle regole:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
```

```
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Per l'`ComplianceResourceTypes`attributo, questo codice JSON limita l'ambito alle risorse del `AWS::EC2::Instance` tipo, quindi AWS Config valuterà solo le istanze EC2 rispetto alla regola. Poiché questa regola è una regola gestita dal cliente, l'`Owner`attributo è impostato su e l'`SourceIdentifier`attributo è impostato sull'ARN della funzione Lambda AWS . `CUSTOM_LAMBDA` L'`SourceDetails`soggetto è obbligatorio. I parametri specificati per l'`InputParameters`attributo vengono passati alla funzione AWS Lambda quando AWS Config la richiama per valutare le risorse rispetto alla regola.

Se il comando ha esito positivo, AWS Config non restituisce alcun output. Per verificare la configurazione della regola, esegui il describe-config-rules comando e specifica il nome della regola.

- Per i dettagli sull'API, consulta PutConfigRule in AWS CLI Command Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """
```

```
    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Per i dettagli sull'API, consulta PutConfigRule in AWS SDK for Python (Boto3) API Reference.

Eliminazione delle regole

I seguenti esempi di codice mostrano come utilizzare. `DeleteConfigRule`

CLI

AWS CLI

Per eliminare una regola di AWS Config

Il comando seguente elimina una regola AWS Config denominata: `MyConfigRule`

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Per i dettagli sull'API, consulta DeleteConfigRule in AWS CLI Command Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.
```

```
        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- Per i dettagli sull'API, consulta DeleteConfigRule in AWS SDK for Python (Boto3) API Reference.

Attivazione della valutazione proattiva ()AWS CLI

Puoi utilizzare la valutazione proattiva per valutare le risorse prima che vengano implementate. Ciò consente di valutare se un insieme di proprietà della risorsa, se utilizzato per definire una AWS risorsa, sarebbe CONFORME o NON CONFORME, in base all'insieme di regole proattive che hai nel tuo account nella tua regione.

Lo schema del tipo di risorsa indica le proprietà di una risorsa. Puoi trovare lo schema del tipo di risorsa nelle "estensioni AWS pubbliche" all'interno del AWS CloudFormation registro o con il seguente comando CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Per ulteriori informazioni, consulta Gestione delle estensioni tramite il AWS CloudFormation registro e il riferimento ai tipi di AWS risorse e proprietà nella Guida per l' AWS CloudFormation utente.

> **Note**
>
> Le regole proattive non correggono le risorse contrassegnate come NON_COMPLIANT e non ne impediscono l'implementazione.

Per attivare la valutazione proattiva

Usa il comando `put-config-rule` e abilita `PROACTIVE` per `EvaluationModes`.

Dopo aver attivato la valutazione proattiva, puoi utilizzare il comando CLI start-resource-evaluation e il comando CLI get-resource-evaluation-summary per verificare se le risorse specificate in questi comandi verrebbero contrassegnate come NON_COMPLIANT dalle regole proattive del tuo account nella tua regione.

Ad esempio, inizia con il comando start-resource-evaluation:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Viene visualizzato `ResourceEvaluationId` nell'output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Quindi, usa `ResourceEvaluationId` con get-resource-evaluation-summary per verificare il risultato della valutazione:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Riceverai un output simile al seguente:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
```

```
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Per visualizzare informazioni aggiuntive sul risultato della valutazione, ad esempio quale regola ha contrassegnato una risorsa come NON_COMPLIANT, utilizza il comando dell'interfaccia a riga di comando get-compliance-details-by-resource.

> **Note**
>
> Per un elenco di regole gestite che AWS Config supportano la valutazione proattiva, vedi Elenco delle regole gestite per modalità di valutazione.

Attivazione della valutazione proattiva (API)

Puoi utilizzare la valutazione proattiva per valutare le risorse prima che vengano implementate. Ciò ti consente di valutare se un insieme di proprietà della risorsa, se utilizzato per definire una AWS risorsa, sarebbe CONFORME o NON CONFORME, in base all'insieme di regole proattive che hai nel tuo account nella tua regione.

Lo schema del tipo di risorsa indica le proprietà di una risorsa. Puoi trovare lo schema del tipo di risorsa nelle "estensioni AWS pubbliche" all'interno del AWS CloudFormation registro o con il seguente comando CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Per ulteriori informazioni, consulta Gestione delle estensioni tramite il AWS CloudFormation registro e il riferimento ai tipi di AWS risorse e proprietà nella Guida per l' AWS CloudFormation utente.

> **Note**
>
> Le regole proattive non correggono le risorse contrassegnate come NON_COMPLIANT e non ne impediscono l'implementazione.

Per attivare la valutazione proattiva per una regola

Usa l'azione PutConfigRegola e abilita `PROACTIVE` per`EvaluationModes`.

Dopo aver attivato la valutazione proattiva, puoi utilizzare l'API di StartResourcevalutazione e l'GetResourceEvaluationSummaryAPI per verificare se le risorse specificate in questi comandi verranno contrassegnate come NON_COMPLIANT dalle regole proattive del tuo account nella tua regione. Ad esempio, inizia con l'API: StartResourceEvaluation

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Viene visualizzato `ResourceEvaluationId` nell'output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Quindi, utilizza `ResourceEvaluationId` con l' GetResourceEvaluationSummary API per verificare il risultato della valutazione:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Riceverai un output simile al seguente:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
```

```
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Per visualizzare informazioni aggiuntive sul risultato della valutazione, ad esempio la regola che ha contrassegnato una risorsa come NON_COMPLIANT, utilizza l'API Resource. GetCompliance DetailsBy

> **Note**
>
> Per un elenco di regole gestite che supportano la valutazione proattiva, vedi Elenco delle regole gestite per modalità di valutazione. AWS Config

Invio delle valutazioni della regola a Security Hub

Dopo aver aggiunto una AWS Config regola, puoi anche inviare le valutazioni delle regole a AWS Security Hub. L'integrazione tra AWS Config e Security Hub consente di valutare e correggere le valutazioni delle regole insieme ad altri errori di configurazione e problemi di sicurezza.

Invio delle valutazioni della regola a Security Hub

Per inviare le valutazioni delle regole a Security Hub AWS Config, devi prima configurare AWS Security Hub e quindi aggiungere almeno una regola AWS Config gestita o personalizzata. Dopodiché, inizia AWS Config immediatamente a inviare le valutazioni delle regole a Security Hub. Security Hub arricchisce le valutazioni della regola e le trasforma in esiti di Security Hub.

Per ulteriori informazioni su questa integrazione, consulta Integrazioni AWS di servizi disponibili nella Guida per l' AWS Security Hub utente.

Valutare le risorse con le regole AWS Config

Quando si creano regole personalizzate o si utilizzano regole gestite, AWS Config valuta le risorse in base a tali regole. Puoi anche decidere di eseguire valutazioni on demand per le risorse a fronte delle regole. Ad esempio, ciò è utile quando si crea una regola personalizzata e si desidera verificare che

AWS Config stia valutando correttamente le risorse o per identificare se esiste un problema con la logica di valutazione della funzione. AWS Lambda

Esempio

1. Crea una regola personalizzata che valuta se gli utenti IAM dispongono di chiavi di accesso attive.
2. AWS Config valuta le risorse in base alla regola personalizzata.
3. Nell'account è presente un utente IAM che non dispone di una chiave di accesso attiva. La regola non contrassegna correttamente questa risorsa come NON_COMPLIANT.
4. Correggi il problema e avvii nuovamente la valutazione.
5. Dopo la correzione, la regola valuta correttamente le risorse e contrassegna la risorsa dell'utente IAM come NON_COMPLIANT.

Quando aggiungi una regola al tuo account, puoi specificare in che momento del processo di creazione e gestione delle risorse desideri AWS Config valutare le tue risorse. Il processo di creazione e gestione delle risorse è noto come provisioning delle risorse. Scegliete la modalità di valutazione per specificare quando, in questo processo, desiderate AWS Config valutare le vostre risorse.

A seconda della regola, è AWS Config possibile valutare le configurazioni delle risorse prima che una risorsa venga distribuita, dopo la distribuzione di una risorsa o entrambe le cose. La valutazione di una risorsa prima che venga implementata è chiamata valutazione proattiva. La valutazione di una risorsa dopo che è stata implementata è chiamata valutazione dei test.

Modalità proattiva

Utilizza la valutazione proattiva per valutare le risorse prima che vengano implementate. Ciò consente di valutare se un insieme di proprietà delle risorse, se utilizzato per definire una AWS risorsa, sarebbe CONFORME o NON_COMPLIANT, in base all'insieme di regole proattive che hai nel tuo account nella tua regione.

Lo schema del tipo di risorsa indica le proprietà di una risorsa. Puoi trovare lo schema del tipo di risorsa nelle "estensioni AWS pubbliche" all'interno del AWS CloudFormation registro o con il seguente comando CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Per ulteriori informazioni, consulta Gestione delle estensioni tramite il AWS CloudFormation registro e il riferimento ai tipi di AWS risorse e proprietà nella Guida per l' AWS CloudFormation utente.

> **Note**
>
> Le regole proattive non correggono le risorse contrassegnate come NON_COMPLIANT e non ne impediscono l'implementazione.

Valutazione delle risorse

Per attivare la valutazione proattiva

1. Accedere AWS Management Console e aprire la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Nel AWS Management Console menu, verifica che il selettore della regione sia impostato su una regione che supporta AWS Config le regole. Per un elenco delle regioni AWS supportate, consulta Regioni ed endpoint AWS Config in Riferimenti generali di Amazon Web Services.
3. Nel riquadro di navigazione di sinistra seleziona Rules (Regole). Per un elenco di regole gestite che supportano la valutazione proattiva, vedi Elenco delle regole AWS Config gestite per modalità di valutazione.
4. Seleziona una regola e scegli Modifica regola per la regola che desideri aggiornare.
5. In Modalità di valutazione, scegli Attivazione della valutazione proattiva per eseguire valutazioni sulle impostazioni di configurazione delle risorse prima che vengano implementate.
6. Selezionare Salva.

> **Note**
>
> Puoi anche attivare la valutazione proattiva utilizzando il `put-config-rule`comando e abilitando `PROACTIVE` for `EvaluationModes` o utilizzando l'PutConfigRuleazione e l'abilitazione `PROACTIVE` per. `EvaluationModes`

Dopo aver attivato la valutazione proattiva, puoi utilizzare l'StartResourceEvaluationAPI e l'GetResourceEvaluationSummaryAPI per verificare se le risorse specificate in questi comandi verranno contrassegnate come NON_COMPLIANT dalle regole proattive del tuo account nella tua regione.

Ad esempio, inizia con l'API: StartResourceEvaluation

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Viene visualizzato `ResourceEvaluationId` nell'output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Quindi, utilizza `ResourceEvaluationId` con l' GetResourceEvaluationSummary API per verificare il risultato della valutazione:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Riceverai un output simile al seguente:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Per visualizzare informazioni aggiuntive sul risultato della valutazione, ad esempio la regola che ha contrassegnato una risorsa come NON_COMPLIANT, utilizza l'API. GetComplianceDetailsByResource

Modalità di test

Utilizza la valutazione di test per valutare le risorse che sono già state implementate. Ciò consente di valutare le impostazioni di configurazione delle risorse esistenti.

Valutazione delle risorse (console)

1. Accedi e apri la console all'indirizzo https://console.aws.amazon.com/config/ AWS Management Console . AWS Config
2. Nel AWS Management Console menu, verifica che il selettore della regione sia impostato su una regione che supporta AWS Config le regole. Per un elenco delle regioni supportate, consultaRegioni ed endpoint di AWS Config nei Riferimenti generali di Amazon Web Services.
3. Nel pannello di navigazione, scegli Regole. Nella pagina Regole sono riportati il nome, l'azione di riparazione associata e lo stato di conformità di ogni regola.
4. Scegli una regola dalla tabella.
5. Dall'elenco a discesa Azioni, scegli Rivaluta.
6. AWS Config inizia a valutare le risorse in base alla tua regola.

> **Note**
>
> È possibile rivalutare una regola una volta al minuto. È necessario attendere il AWS Config completamento della valutazione della regola prima di iniziare un'altra valutazione. Non puoi eseguire una valutazione mentre la regola viene aggiornata o se viene eliminata.

Valutazione delle risorse (CLI)

- Utilizza il comando start-config-rules-evaluation:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName
```

AWS Config inizia a valutare le configurazioni delle risorse registrate rispetto alla regola. Nella richiesta si possono anche specificare più regole:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

Valutazione delle risorse (API)

Usa l'azione StartConfigRulesEvaluation.

Eliminazione dei risultati della valutazione dalle regole AWS Config

Dopo che AWS Config valuta la tua regola, puoi visualizzare i risultati della valutazione nella pagina (Rules) Regole o nella pagina Rules details (Dettagli regola) per la regola. Se i risultati della valutazione non sono corretti o se desideri una nuova valutazione, puoi eliminare l'attuale valutazione dei risultati per la regola. Ad esempio, se la regola stava erroneamente valutando le risorse o se hai recentemente eliminato le risorse dall'account, puoi eliminare i risultati della valutazione e quindi eseguire una nuova valutazione.

Eliminazione dei risultati della valutazione (console)

1. Accedi alla AWS Management Console e aprire la console di AWS Config all'indirizzo https://console.aws.amazon.com/config/.
2. Nel AWS Management Console menu, verifica che il selettore della regione sia impostato su una AWS regione che supporta AWS Config le regole. Per l'elenco delle regioni supportate, consulta AWS ConfigRegioni ed endpoint in. Riferimenti generali di Amazon Web Services
3. Nel pannello di navigazione, scegli Rules (Regole). La pagina Regole mostra il nome, l'azione correttiva associata e lo stato di conformità di ogni regola.
4. Scegliete una regola dalla tabella.
5. Dall'elenco a discesa Azioni, scegli Elimina risultati.
6. Quando richiesto, digita Elimina (questa voce fa distinzione tra maiuscole e minuscole), quindi scegli Elimina. Dopo aver eliminato una valutazione, non è possibile recuperarla.
7. Dopo l'eliminazione dei risultati della valutazione, puoi avviare manualmente una nuova valutazione.

Eliminazione dei risultati della valutazione (CLI)

- Utilizza il comando delete-evaluation-results.

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

AWS Config elimina risultati della valutazione per la regola.

Eliminazione dei risultati della valutazione (API)

Usa l'azione DeleteEvaluationResults.

Gestione AWS Config delle regole per tutti gli account dell'organizzazione

> **Important**
>
> Le regole organizzative possono essere create soltanto tramite l'API o l'interfaccia a riga di comando. Questa operazione non è supportata nella AWS Config console.

AWS Config consente di gestire AWS Config le regole Account AWS all'interno di un'organizzazione. È possibile:

- Crea, aggiorna ed elimina AWS Config le regole in modo centralizzato per tutti gli account dell'organizzazione.
- Implementa un insieme comune di AWS Config regole per tutti gli account e specifica gli account in cui non devono essere create AWS Config regole.
- Utilizza le API dell'account di gestione AWS Organizations per applicare la governance assicurandoti che le AWS Config regole sottostanti non siano modificabili dagli account dei membri dell'organizzazione.

Considerazioni

Per le implementazioni in diverse regioni

La chiamata API per distribuire regole e pacchetti di conformità tra gli account è specifica della regione. AWS A livello di organizzazione, è necessario modificare il contesto della chiamata API su un'altra regione se desideri implementare le regole in altre regioni. Ad esempio, per implementare una regola negli Stati Uniti orientali (Virginia settentrionale), modifica la regione in Stati Uniti orientali (Virginia settentrionale) e quindi chiama `PutOrganizationConfigRule`.

Per gli account all'interno di un'organizzazione

Se un nuovo account entra a far parte di un'organizzazione, la regola o il pacchetto di conformità vengono implementati in quell'account. Quando un account lascia un'organizzazione, la regola o il pacchetto di conformità vengono rimossi.

Se implementi una regola o un pacchetto di conformità organizzativi in un account amministratore dell'organizzazione e quindi stabilisci un amministratore delegato e implementi una regola o un pacchetto di conformità organizzativi nell'account amministratore delegato, non potrai visualizzare la regola o il pacchetto di conformità organizzativi nell'account amministratore dell'organizzazione dall'account amministratore delegato o visualizzare la regola o il pacchetto di conformità organizzativi nell'account amministratore delegato dall'account amministratore dell'organizzazione. Le DescribeOrganizationConformancePacksAPI DescribeOrganizationConfigRulese possono solo visualizzare e interagire con le risorse relative all'organizzazione che sono state distribuite dall'account che chiama tali API.

Meccanismo di tentativi per i nuovi account aggiunti a un'organizzazione

Se non è disponibile un registratore, l'implementazione delle regole e dei pacchetti di conformità organizzativi esistenti viene ritentata solo per 7 ore dopo l'aggiunta di un account all'organizzazione. È necessario creare un registratore, se non ne esiste uno, entro 7 ore dall'aggiunta di un account all'organizzazione.

Account di gestione dell'organizzazione, amministratori delegati e ruoli collegati ai servizi

Se utilizzi un account di gestione dell'organizzazione e intendi utilizzare un amministratore delegato per la distribuzione organizzativa, tieni presente che questo AWS Config non creerà automaticamente il ruolo collegato al servizio (SLR). È necessario creare manualmente il ruolo collegato al servizio (SLR) separatamente utilizzando IAM.

Se non disponi di una reflex per il tuo account di gestione, non sarai in grado di distribuire risorse su quell'account da un account amministratore delegato. Sarete comunque in grado di distribuire AWS Config le regole agli account dei membri dagli account di gestione e dagli account di amministratore

delegato. Per ulteriori informazioni, consulta Using service-linked roles nella Guida per l'utente AWS Identity and Access Management (IAM).

Implementazione

Per informazioni su come eseguire l'integrazione AWS Config con AWS Organizations, consulta AWS Config e AWS Organizations nella Guida per l'AWS Organizations utente. Assicurati che AWS Config la registrazione sia attiva prima di utilizzare le seguenti API per gestire AWS Config le regole Account AWS all'interno di un'organizzazione:

- PutOrganizationConfigRule, aggiunge o aggiorna la regola di configurazione dell'organizzazione per l'intera organizzazione, valutando se le AWS risorse sono conformi alle configurazioni desiderate.
- DescribeOrganizationConfigRules, restituisce un elenco di regole di configurazione dell'organizzazione.
- GetOrganizationConfigRuleDetailedStatus, restituisce lo stato dettagliato di ogni account membro all'interno di un'organizzazione per una determinata regola di configurazione dell'organizzazione.
- GetOrganizationCustomRulePolicy, restituisce la definizione della politica contenente la logica per la regola di politica personalizzata di configurazione dell'organizzazione.
- DescribeOrganizationConfigRuleStati, fornisce lo stato di implementazione delle regole di configurazione dell'organizzazione per un'organizzazione.
- DeleteOrganizationConfigRule, elimina la regola di configurazione dell'organizzazione specificata e tutti i relativi risultati di valutazione da tutti gli account membri dell'organizzazione.

Supporto nelle regioni

La distribuzione AWS Config delle regole tra gli account dei membri di un' AWS organizzazione è supportata nelle seguenti regioni.

Nome della regione	Regione	Endpoint	Protocollo	
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Stati Uniti occidentali (California settentrionale)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Asia Pacifico (Giacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pacifico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacifico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacifico (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacifico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Centrale)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europa (Francoforte)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londra)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Parigi)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Sud America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Correzione delle risorse non conformi con regole AWS Config

AWS Config consente di correggere le risorse non conformi che vengono valutate da. Regole di AWS Config AWS Config applica la riparazione utilizzando i documenti di automazione.AWS Systems Manager Questi documenti definiscono le azioni da eseguire sulle risorse non conformi AWS valutate da. Regole di AWS ConfigÈ possibile associare documenti SSM utilizzando la AWS Management Console o le API.

AWS Config fornisce una serie di documenti di automazione gestiti con azioni correttive. È inoltre possibile creare e associare documenti di automazione personalizzati alle AWS Config regole.

Per applicare la riparazione alle risorse non conformi, puoi scegliere l'azione di riparazione che desideri associare da un elenco precompilato o creare azioni di riparazione personalizzate utilizzando i documenti SSM. AWS Config fornisce un elenco di azioni correttive consigliate in. AWS Management Console

In AWS Management Console, è possibile scegliere di correggere manualmente o automaticamente le risorse non conformi associando le azioni di riparazione alle regole. AWS Config Con tutte le operazioni di correzione, puoi scegliere la correzione manuale o automatica.

Argomenti

- Prerequisito
- Configurazione della correzione manuale (console)
- Configurazione della correzione automatica (console)
- Eliminare l'operazione di correzione (console)
- Gestione della correzione (API)
- Supporto nelle regioni

Prerequisito

Prima di avviare il processo di correzione su risorse non conformi, è necessario selezionare una regola e configurare il processo di correzione (manuale o automatico) per la regola.

Configurazione della correzione manuale (console)

1. Accedi e apri la console all'indirizzo https://console.aws.amazon.com/config/ AWS Management Console . AWS Config
2. Scegli Regole sulla sinistra e quindi, nella pagina Regole, scegli Aggiungi regola per aggiungere nuove regole all'elenco delle regole

   Per le regole esistenti, seleziona la regola non conforme dall'elenco e scegli l'elenco a discesa Azioni.
3. Dall'elenco a discesa Azioni, scegli Gestisci riparazione. Seleziona "Riparazione manuale", quindi scegli l'azione di riparazione appropriata dall'elenco consigliato.

   > **Note**
   >
   > Puoi gestire solo le correzioni per le regole non collegate ai AWS Config servizi. Per ulteriori informazioni, consulta Regole AWS collegate ai servizi.

A seconda dell'operazione selezionata, vengono visualizzati dei parametri specifici o non viene visualizzato alcun parametro.

4. (Facoltativo): se si desidera trasferire l'ID delle risorse non conformi sull'operazione di correzione, selezionare Resource ID parameter (Parametro ID risorsa). Se selezionato, in fase di runtime il parametro viene sostituito con l'ID della risorsa da correggere.

   Ogni parametro dispone di un valore statico o di un valore dinamico. Se non selezioni un parametro dell'ID di risorsa dall'elenco a discesa, puoi inserire valori per ogni chiave. In caso contrario, puoi inserire valori per tutte le altre chiavi, tranne per il parametro dell'ID di risorsa selezionato.

5. Selezionare Salva. Viene visualizzata la pagina Rules (Regole).

Per la risoluzione dei problemi relativi alle azioni di riparazione non riuscite, è possibile eseguire il AWS comando Command Line Interface `describe-remediation-execution-status` per ottenere una visualizzazione dettagliata dell'esecuzione della riparazione per un insieme di risorse. I dettagli includono lo stato, i timestamp per le fasi di esecuzione della correzione ed eventuali messaggi di errore per le fasi non riuscite.

Configurazione della correzione automatica (console)

1. Accedere AWS Management Console e aprire la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Scegliere Regole sulla sinistra e quindi nella pagina Regole scegliere Aggiungi regola per aggiungere nuove regole all'elenco.

   Per le regole esistenti, seleziona la regola non conforme dall'elenco e scegli l'elenco a discesa Azioni.

3. Dall'elenco a discesa Azioni, scegli Gestisci riparazione. Seleziona "Riparazione automatica", quindi scegli l'azione di riparazione appropriata dall'elenco consigliato.

> **Note**
>
> Puoi gestire solo le correzioni per le regole non collegate ai AWS Config servizi. Per ulteriori informazioni, consulta Regole AWS collegate ai servizi.

A seconda dell'operazione selezionata, vengono visualizzati dei parametri specifici o non viene visualizzato alcun parametro.

4. Scegliere Auto remediation (Correzione automatica) per correggere automaticamente le risorse non conformi.

   Se una risorsa non è ancora conforme dopo la riparazione automatica, puoi impostare la regola per riprovare la riparazione automatica. Immettere i nuovi tentativi e i secondi desiderati.

   > **Note**
   >
   > Esistono dei costi associati all'esecuzione ripetuta di uno script di correzione. I nuovi tentativi si verificano solo se la riparazione non riesce e funziona entro il periodo di tempo specificato; ad esempio 5 nuovi tentativi in 300 secondi.

5. (Facoltativo): se si desidera trasferire l'ID delle risorse non conformi sull'operazione di correzione, selezionare Resource ID parameter (Parametro ID risorsa). Se selezionato, in fase di runtime il parametro viene sostituito con l'ID della risorsa da correggere.

   Ogni parametro dispone di un valore statico o di un valore dinamico. Se non selezioni un parametro dell'ID di risorsa dall'elenco a discesa, puoi inserire valori per ogni chiave. In caso contrario, puoi inserire valori per tutte le altre chiavi, tranne per il parametro dell'ID di risorsa selezionato.

6. Selezionare Salva. Viene visualizzata la pagina Rules (Regole).

Per la risoluzione dei problemi relativi alle azioni di riparazione non riuscite

Per la risoluzione dei problemi relativi alle azioni di riparazione non riuscite, è possibile eseguire il AWS comando Command Line Interface `describe-remediation-execution-status` per ottenere una visualizzazione dettagliata dell'esecuzione della riparazione per un insieme di risorse. I dettagli includono lo stato, i timestamp per le fasi di esecuzione della correzione ed eventuali messaggi di errore per le fasi non riuscite.

La riparazione automatica può essere avviata anche per le risorse conformi

Se abiliti la riparazione automatica per una AWS Config regola specifica utilizzando l'API PutRemediationConfigurations o la AWS Config console, avvia il processo di riparazione per tutte le risorse non conformi per quella regola specifica. Il processo di riparazione automatica si basa

sull'istantanea dei dati di conformità che viene acquisita su base periodica. Qualsiasi risorsa non conforme che viene aggiornata tra la pianificazione delle istantanee continuerà a essere risolta in base all'ultimo snapshot dei dati di conformità noto.

Ciò significa che in alcuni casi è possibile avviare la riparazione automatica anche per le risorse conformi, poiché il processore bootstrap utilizza un database che può avere risultati di valutazione non aggiornati basati sull'ultima istantanea dei dati di conformità nota.

Eliminare l'operazione di correzione (console)

Per eliminare una regola è necessario eliminare prima l'operazione di correzione associata alla regola.

1. Accedere e aprire la console all'indirizzo https://console.aws.amazon.com/config/. AWS Management ConsoleAWS Config
2. Scegli Regole sulla sinistra e quindi, nella pagina Regole, seleziona la regola dall'elenco e scegli Visualizza dettagli.
3. Nella pagina *Nome della regola*, vai alla sezione Operazione di riparazione. Espandi la sezione per visualizzare ulteriori dettagli.
4. Nella sezione Operazione di riparazione, scegli Elimina e conferma l'azione di eliminazione.

   > **Note**
   >
   > L'eliminazione non viene eseguita se l'azione di riparazione è in corso. Se selezioni Elimina operazione di riparazione, non potrai recuperarla. L'eliminazione di un'azione di riparazione non elimina la regola associata.

   Se viene eliminata un'azione di riparazione, il campo Parametro di risorsa ID sarà vuoto e mostrerà N/A. Nella pagina Regole, nella colonna Operazione di riparazione viene visualizzato Senza impostazioni per la regola associata.

Gestione della correzione (API)

Correzione manuale

Utilizza le seguenti azioni AWS Config API per gestire la riparazione:

- DeleteRemediationConfigurazione, elimina la configurazione di riparazione.
- DescribeRemediationConfigurazioni, restituisce i dettagli di una o più configurazioni di riparazione.
- DescribeRemediationExecutionStatus, fornisce una visualizzazione dettagliata dell'esecuzione della riparazione per un insieme di risorse, tra cui lo stato, i timestamp relativi alle fasi di esecuzione della riparazione ed eventuali messaggi di errore relativi alle fasi non riuscite.
- PutRemediationConfigurazioni, aggiunge o aggiorna la configurazione di riparazione con una AWS Config regola specifica con l'obiettivo o l'azione selezionati.
- StartRemediationEsecuzione, esegue una riparazione su richiesta per AWS Config le regole specificate rispetto all'ultima configurazione di riparazione nota.

Correzione automatica

Utilizza le seguenti azioni AWS Config API per gestire la riparazione automatica:

- PutRemediationEccezioni, aggiunge una nuova eccezione o aggiorna un'eccezione esistente per una risorsa specifica con una regola specifica. AWS Config
- DescribeRemediationEccezioni, restituisce i dettagli di una o più eccezioni di correzione.
- DeleteRemediationEccezioni, elimina una o più eccezioni di riparazione menzionate nelle chiavi di risorsa.

Supporto nelle regioni

Attualmente, le azioni correttive per AWS Config Rules sono supportate nelle seguenti aree:

Nome della regione	Regione	Endpoint	Protocollo
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo	
Stati Uniti occidentali (California settentrionale)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
Asia Pacifico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Asia Pacific (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
Asia Pacifico (Giacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Asia Pacifico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacifico (Osaka-Locale)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacifico (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacifico (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacifico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Centrale)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Canada occidentale (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Europa (Francoforte)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londra)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milano)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Parigi)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spagna)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zurigo)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israele (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Medio Oriente (Bahrein)	me-south-1	config.me-south-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Medio Oriente (Emirati Arabi Uniti)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Sud America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Risoluzione dei problemi

Controlla i seguenti problemi per risolvere i problemi se non riesci a eliminare una AWS Config regola o ricevi un errore simile al seguente: «Si è verificato un errore con». AWS Config

L'entità AWS Identity and Access Management (IAM) dispone delle autorizzazioni per l'API DeleteConfigRule

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.

2. Nel riquadro di navigazione scegli Utenti o Ruoli.
3. Scegli l'utente o il ruolo che hai usato per eliminare la AWS Config regola ed espandi le politiche di autorizzazione.
4. Nella scheda Autorizzazioni, scegli JSON.
5. Nel riquadro di anteprima JSON, conferma che la policy IAM consenta le autorizzazioni per l'API Rule. DeleteConfig

Il limite di autorizzazione dell'entità IAM consente l'API DeleteConfigRule

Se l'entità IAM ha un limite di autorizzazioni, assicurati che consenta le autorizzazioni per l'API. DeleteConfigRule

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione scegli Utenti o Ruoli.
3. Scegli l'utente o il ruolo che hai usato per eliminare la AWS Config regola, espandi il limite delle autorizzazioni e quindi scegli JSON.
4. Nel riquadro di anteprima JSON, conferma che la policy IAM consenta le autorizzazioni per l'API Rule. DeleteConfig

> **Warning**
>
> Gli utenti IAM dispongono di credenziali a lungo termine, il che rappresenta un rischio per la sicurezza. Per contribuire a mitigare questo rischio, ti consigliamo di fornire a questi utenti solo le autorizzazioni necessarie per eseguire l'attività e di rimuoverli quando non sono più necessari.

La policy di controllo del servizio (SCP) consente l'API DeleteConfigRule

1. Apri la AWS Organizations console all'indirizzo https://console.aws.amazon.com/organizations/ utilizzando l'account di gestione dell'organizzazione.
2. In Nome account, scegli Account AWS.
3. In Politiche, espandi le politiche di controllo del servizio e prendi nota delle politiche SCP allegate.
4. Nella parte superiore della pagina, scegli Politiche.
5. Seleziona la politica, quindi scegli Visualizza dettagli.

6. Nel riquadro di anteprima JSON, conferma che la policy consenta l'API DeleteConfigRule.

La regola non è una regola collegata al servizio

Quando abiliti uno standard di sicurezza, AWS Security Hub crea automaticamente regole collegate ai servizi. Non è possibile eliminare queste regole collegate al servizio utilizzando AWS Config e il pulsante di eliminazione è disattivato. Per rimuovere una regola collegata al servizio, vedere Disabilitazione di uno standard di sicurezza nella Guida per l'utente di Security Hub.

Non è in corso alcuna azione di riparazione

Non è possibile eliminare AWS Config le regole per le quali sono in corso azioni di riparazione. Segui i passaggi per eliminare l'azione di riparazione associata a quella regola. Quindi, prova a eliminare nuovamente la regola.

> **Important**
>
> Elimina solo le azioni di riparazione che si trovano nello stato di fallimento o di successo.

Pacchetti di conformità

Un pacchetto di conformità è una raccolta di AWS Config regole e azioni correttive che possono essere facilmente implementate come singola entità in un account e in una regione o all'interno di un'organizzazione in. AWS Organizations

I pacchetti di conformità vengono creati con un modello YAML contenente l'elenco delle regole AWS Config gestite o personalizzate e le operazioni di correzione. È inoltre possibile utilizzare AWS Systems Manager documenti (documenti SSM) per archiviare i modelli dei pacchetti di conformità AWS e distribuire direttamente i pacchetti di conformità utilizzando i nomi dei documenti SSM. Puoi distribuire il modello utilizzando la console AWS Config o l' AWS CLI.

Per iniziare rapidamente e valutare il tuo AWS ambiente, utilizza uno dei modelli di conformance pack di esempio. Puoi anche creare un file YAML del pacchetto di conformità da zero basandoti su quanto riportato in Pacchetto di conformità personalizzato.

Argomenti

- Prerequisiti
- Supporto nelle regioni
- AWS Config Controlli di processo all'interno di un pacchetto di conformità
- Modelli di esempio di pacchetto di conformità
- Pacchetti di conformità personalizzati
- Visualizzazione dei dati di conformità nel pannello di controllo dei pacchetti di conformità
- Visualizzazione della timeline della cronologia di conformità dei pacchetti di conformità
- Distribuzione di un pacchetto di conformità utilizzando la console AWS Config
- Distribuzione di un pacchetto di conformità utilizzando l' AWS Command Line Interface
- Gestione dei pacchetti di conformità (API)
- Gestione dei pacchetti di conformità in tutti gli account dell'organizzazione
- Risoluzione dei problemi

Prerequisiti

Prima di implementare il pacchetto di conformità, attiva la registrazione. AWS Config

Inizia la registrazione AWS Config

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Scegliere Settings (Impostazioni) nel riquadro di navigazione.
3. Per avviare la registrazione, in La registrazione è disattivata, scegli Attiva. Quando richiesto, scegli Continua.

Prerequisiti per l'utilizzo di un pacchetto di conformità con correzione

Prima di distribuire pacchetti di conformità utilizzando modelli di esempio con correzione, è necessario creare risorse appropriate come automation assume role e altre AWS risorse in base all'obiettivo di riparazione.

Se hai un ruolo di automazione esistente che usi per la correzione con i documenti SSM, puoi fornire direttamente l'ARN del ruolo. Se hai risorse puoi specificarle nel modello.

> **Note**
>
> Quando implementi un pacchetto di conformità con riparazione in un'organizzazione, occorre specificare l'ID dell'account di gestione dell'organizzazione. In caso contrario, durante l'implementazione del pacchetto di conformità organizzativo, AWS Config sostituisce automaticamente l'ID dell'account di gestione con l'ID dell'account membro.

AWS Config non supporta funzioni AWS CloudFormation intrinseche per il ruolo di esecuzione dell'automazione. È necessario fornire l'ARN esatto del ruolo come stringa.

Per ulteriori informazioni su come passare l'ARN esatto, consulta Modelli di esempio di pacchetto di conformità. Quando usi i modelli di esempio, aggiorna l'ID dell'account e l'ID dell'account di gestione dell'organizzazione.

Prerequisiti per l'utilizzo di un Conformance Pack con una o più regole AWS Config

Prima di distribuire un pacchetto di conformità con una o più AWS Config regole personalizzate, create risorse appropriate come la AWS Lambda funzione e il ruolo di esecuzione corrispondente.

Se disponi di una AWS Config regola personalizzata esistente, puoi fornire direttamente la AWS Lambda funzione ARN of per creare un'altra istanza di quella regola personalizzata come parte del pacchetto.

Se non disponi di una AWS Config regola personalizzata esistente, puoi creare una AWS Lambda funzione e utilizzare l'ARN della funzione Lambda. Per ulteriori informazioni, consulta AWS Config Regole personalizzate.

Se la AWS Lambda funzione è presente in un altro account Account AWS, è possibile creare AWS Config regole con l'autorizzazione appropriata della funzione tra account AWS Lambda . Per ulteriori informazioni, consulta Come gestire centralmente AWS Config le regole in più post Account AWS del blog.

Same account bucket policy

AWS Config Per poter archiviare gli elementi del Conformance Pack, dovrai fornire un bucket Amazon S3 e aggiungere le seguenti autorizzazioni. Per ulteriori informazioni sulla denominazione dei bucket, consulta Regole di denominazione dei bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::delivery-bucket-name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
```

```
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::delivery-bucket-name/[optional] prefix/
AWSLogs/AccountId/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Cross-account bucket policy

AWS Config Per poter archiviare gli elementi del Conformance Pack, dovrai fornire un bucket Amazon S3 e aggiungere le seguenti autorizzazioni. Per ulteriori informazioni sulla denominazione dei bucket, consulta Regole di denominazione dei bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms",
            "PutConformancePack API caller user principal like
 arn:aws:iam::SourceAccountId:user/userName "
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
```

```
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
    {
      "Sid": " AWSConfigConformsBucketReadAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*"
    }
  ]
}
```

> **Note**
>
> Quando implementi pacchetti di conformità per più account, il nome del bucket di consegna Amazon S3 deve iniziare con `awsconfigconforms`.

Prerequisiti per i pacchetti di conformità dell'organizzazione

Specifica l'ARN di un ruolo di esecuzione di automazione per la correzione nel modello se il modello di input hai una configurazione di correzione automatica. Assicurati che in tutti gli account (gestione e membro) di un'organizzazione esista un ruolo con il nome specificato. È necessario creare questo ruolo in tutti gli account prima di chiamare `PutOrganizationConformancePack`. Puoi creare

questo ruolo manualmente o utilizzando gli AWS CloudFormation stack-set per creare questo ruolo in ogni account.

Se il modello utilizza una funzione AWS CloudFormation intrinseca `Fn::ImportValue` per importare una particolare variabile, tale variabile deve essere definita come una `Export Value` in tutti gli account membri di quell'organizzazione.

Per le AWS Config regole personalizzate, vedi Come gestire centralmente AWS Config le regole su più Account AWS blog per configurare le autorizzazioni appropriate.

Policy del bucket di organizzazione:

AWS Config Per poter archiviare gli elementi del Conformance Pack, dovrai fornire un bucket Amazon S3 e aggiungere le seguenti autorizzazioni. Per ulteriori informazioni sulla denominazione dei bucket, consulta Regole di denominazione dei bucket.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                 "s3:GetObject",
                 "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        },
        {
            "Sid": "AllowGetBucketAcl",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetBucketAcl",
```

```
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        }
    ]
}
```

> **Note**
>
> Quando implementi pacchetti di conformità in un'organizzazione, il nome del bucket di consegna Amazon S3 deve iniziare con `awsconfigconforms`.

Supporto nelle regioni

I pacchetti di conformità sono supportati nelle seguenti regioni:

Nome della regione	Regione	Endpoint	Protocollo
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Stati Uniti occidentali (California	us-west-1	config.us-west-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
settentrionale)			
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Asia Pacifico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pacifico (Giacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pacifico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacifico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacifico (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacifico (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Centrale)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europa (Francoforte)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londra)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Parigi)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Medio Oriente (Bahrein)	me-south-1	config.me-south-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Sud America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

La distribuzione dei pacchetti di conformità tra gli account dei membri di un' AWS organizzazione è supportata nelle seguenti regioni.

Nome della regione	Regione	Endpoint	Protocollo
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo	
Stati Uniti occidentali (California settentrionale)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
Asia Pacifico (Giacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Asia Pacifico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
Asia Pacifico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
Asia Pacifico (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	
Asia Pacifico (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Centrale)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europa (Francoforte)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londra)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Parigi)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Sud America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config Controlli di processo all'interno di un pacchetto di conformità

I controlli di processo sono un tipo di AWS Config regola che consente di tenere traccia delle attività esterne e interne che richiedono la verifica nell'ambito dei pacchetti di conformità. Questi controlli possono essere aggiunti a un pacchetto di conformità esistente o a uno nuovo. È possibile tenere traccia di tutta la conformità, inclusi la AWS Config durata e i controlli manuali, in un'unica posizione.

Con i controlli di processo, puoi elencare la conformità dei requisiti e delle azioni in un'unica posizione. I controlli di processo aiutano ad aumentare la copertura dei pacchetti di conformità basati sui regimi di conformità. Puoi espandere ulteriormente il pacchetto di conformità aggiungendo nuovi controlli di processo che tengono traccia dei processi e delle azioni che richiedono la verifica e il monitoraggio manuali. Ciò consente al Conformance Pack di diventare il modello che fornisce dettagli sulla AWS Config durata e sui processi manuali per un regime di conformità.

Puoi monitorare e gestire la conformità dei processi non associati alle modifiche alla configurazione delle risorse all'interno di pacchetti di conformità come controlli di processo Ad esempio, puoi aggiungere un controllo di processo per tenere traccia del requisito di conformità PCI-DSS per archiviare il backup dei supporti in una posizione esterna. Potrai valutare manualmente la

conformità di questo requisito in base alle linee guida PCI-DSS o secondo le indicazioni della tua organizzazione.

Disponibilità regionale: i controlli dei processi con i pacchetti di conformità sono disponibili Regioni AWS ovunque AWS Config siano disponibili i pacchetti di conformità. Per ulteriori informazioni, consulta Supporto nelle regioni.

Argomenti

- Modello di pacchetto di conformità di esempio per la creazione di controlli di processo
- Inclusione dei controlli di processo in un pacchetto di conformità
- Modifica dello stato di conformità di un controllo di processo
- Visualizzazione e modifica del controllo di processo (console)

Modello di pacchetto di conformità di esempio per la creazione di controlli di processo

```
################################################################################
#
#  Conformance Pack template for process check
#
################################################################################
Resources:
  AWSConfigProcessCheck:
    Properties:
      ConfigRuleName: RuleName
      Description: Description of Rule
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

Visualizza due modelli di esempio, il modello Best practice operative per CIS AWS Foundations Benchmark v1.4 Level 1 e il modello Best practice operative per CIS AWS Foundations Benchmark v1.4 Level 2 .

Inclusione dei controlli di processo in un pacchetto di conformità

1. Aggiungi un controllo di processo nel modello del pacchetto di conformità. Fai riferimento al modello di esempio precedente.

```
Resources:
  ConfigEnabledAllRegions:
    Properties:
      ConfigRuleName: Config-Enabled-All-Regions
      Description: Ensure AWS Config is enabled in all Regions.
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

2. Inserisci il nome per il controllo di processo.
3. Inserisci la descrizione per il controllo di processo.
4. Implementa il pacchetto di conformità dalla Console di gestione AWS. Per ulteriori informazioni, consulta Distribuzione di un pacchetto di conformità utilizzando la console AWS Config.

> **Note**
>
> Puoi implementare i pacchetti di conformità anche tramite l'Interfaccia della linea di comando (AWS CLI). Per ulteriori informazioni, consulta Distribuzione di un pacchetto di conformità utilizzando l' AWS Command Line Interface.

Modifica dello stato di conformità di un controllo di processo

Modifica dello stato di conformità di un controllo di processo (console)

Per modificare lo stato di conformità di un controllo del processo (console)

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Vai alla pagina AWS Config delle regole.
3. Scegli il nome del controllo di processo che hai specificato nel modello insieme all'identificatore nel pacchetto di conformità.

> **Note**
>
> Tutti i controlli di processo dello stesso pacchetto di conformità hanno lo stesso suffisso.

4. Nella pagina dei dettagli della regola, non è possibile modificare la regola, ma è possibile modificarne la conformità. Nella sezione Conformità manuale, scegli Modifica della conformità.
5. Scegli la conformità appropriata nell'elenco a discesa.
6. (Facoltativo) Inserisci una descrizione per lo stato di conformità.
7. Selezionare Salva.

Modifica dello stato di conformità di un controllo di processo (CLI)

Per modificare lo stato di conformità di un controllo del processo (CLI)

Puoi aggiornare la conformità dei controlli di processo all'interno di un pacchetto di conformità utilizzando l'Interfaccia della linea di comando AWS (AWS CLI).

Per installarlo AWS CLI sul tuo computer locale, consulta Installazione dell'AWS CLI nella Guida per l'AWS CLI utente.

Se necessario, digita `AWS Config ure` per configurare l'utilizzo AWS CLI di una AWS regione in cui sono disponibili pacchetti di AWS Config conformità.

1. Apri un prompt dei comandi o una finestra del terminale.
2. Immettete il seguente comando per aggiornare la conformità di un processo`Account ID`, controllate dove si `ComplianceResourceId` trova e includete il nome della regola.

```
aws configservice put-external-evaluation --config-rule-
name process-check-rule-name  --external-evaluation
 ComplianceResourceType=AWS::::Account,ComplianceResourceId=Account
 ID,ComplianceType=NON_COMPLIANT,OrderingTimestamp=2020-12-17T00:10:00.000Z
```

3. Premere Invio per eseguire il comando.

Modifica dello stato di conformità di un controllo di processo (API)

Per modificare lo stato di conformità di un controllo di processo (API)

Una volta completata l'implementazione, per aggiornare le valutazioni e la conformità dei controlli di processo, utilizza l'API `PutExternalEvaluation`. Per ulteriori informazioni, consulta PutExternalValutazione.

Visualizzazione e modifica del controllo di processo (console)

Puoi visualizzare i controlli di processo solo dopo aver aggiunto uno stato di conformità ai controlli di processo. Scegli il pacchetto di conformità specifico per visualizzare tutti i controlli di processo in quel pacchetto di conformità. Qui è possibile visualizzare un elenco di controlli di processo conformi e non conformi.

Trattandosi di una regola collegata al servizio, non è possibile modificare il controllo di processo tramite la pagina dei dettagli della regola.

> **Note**
>
> Tuttavia, è possibile aggiornare la conformità del controllo del processo selezionando Modifica conformità e selezionando il valore appropriato tra Conforme, Non conforme o Non applicabile.

Puoi modificare o eliminare un controllo di processo dal pacchetto di conformità in cui sono stati aggiunti i controlli di processo.

Modelli di esempio di pacchetto di conformità

Ecco i modelli YAML del pacchetto di conformità che vedi nella console. AWS Config Nel modello del pacchetto di conformità è possibile utilizzare una o più regole di configurazione e operazioni di correzione AWS Config. Le regole AWS Config elencate nel pacchetto di conformità possono essere regole AWS Config gestite e/o regole AWS Config personalizzate. Puoi scaricare tutti i modelli di conformance pack da. GitHub

> **Important**
>
> I pacchetti di conformità forniscono un framework di conformità generico che consente di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando

regole AWS Config gestite o personalizzate e azioni di correzione AWS Config. I modelli di esempio del pacchetto di conformità AWS consentono di creare pacchetti di conformità personalizzati con regole, parametri di input e azioni correttive diverse o aggiuntive adatte al proprio ambiente. I modelli di esempio, inclusi quelli relativi agli standard di conformità e ai benchmark di settore, non sono progettati per garantire la conformità con uno standard di governance specifico. Non possono né sostituire gli sforzi interni né garantire il superamento di una valutazione di conformità.

> **Note**
>
> Si consiglia di esaminare le regole disponibili nella regione in cui si distribuisce un pacchetto di conformità (Elenco delle regole AWS Config gestite per disponibilità regionale) e di modificare il modello per le regole non ancora disponibili in quella regione prima della distribuzione.

Argomenti

- AWSPacchetto di conformità Control Tower Detective Guardrails
- Best practice operative per ABS CCIG 2.0 Material Workloads
- Best practice operative per ABS CCIG 2.0 Standard Workloads
- Best practice operative per ACSC Essentials 8
- Best practice operative per ACSC ISM
- Best practice operative per IA e ML
- Best practice operative per Gateway Amazon API
- Best practice operative per Amazon CloudWatch
- Best practice operative per Amazon DynamoDB
- Best practice operative per Amazon S3
- Best practice operative per APRA CPG 234
- Best practice operative per la gestione degli asset
- Best practice operative per AWS Backup
- Best practice operative per la gestione delle AWS identità e degli accessi
- Best practice operative per AWS Well-Architected Framework Reliability Pillar

- Best practice operative per AWS Well-Architected Framework Security Pillar
- Best practice operative per BCP e DR
- Best practice operative per BNM RMiT
- Best practice operative per il Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile
- Best practice operative per CIS AWS Foundations Benchmark v1.4 Level 1
- Best practice operative per CIS AWS Foundations Benchmark v1.4 Level 2
- Best practice operative per CIS Critical Security Controls v8 IG1
- Best practice operative per CIS Critical Security Controls v8 IG2
- Best practice operative per CIS Critical Security Controls v8 IG3
- Best practice operative per CIS Top 20
- Best practice operative per CISA Cyber Essentials
- Best practice operative per Criminal Justice Information Services (CJIS)
- Best practice operative per CMMC – Livello 1
- Best practice operative per CMMC – Livello 2
- Best practice operative per CMMC – Livello 3
- Best practice operative per CMMC – Livello 4
- Best practice operative per CMMC – Livello 5
- Best practice operative per CMMC – Livello 1
- Best practice operative per CMMC – Livello 2
- Best practice operative per servizi di calcolo
- Best practice operative per la resilienza dei dati
- Best practice operative per servizi di database
- Best practice operative per data lake e servizi di analisi
- Best practice operative per DevOps
- Best practice operative per EC2
- Best practice operative per la crittografia e la gestione delle chiavi
- Best practice operative per la guida alla cibersicurezza dell'ENISA per le PMI
- Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello basso

- Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello medio
- Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello alto
- Best practice operative per FDA Titolo 21 CFR Parte 11
- Best practice operative per FedRAMP (Low)
- Best practice operative per FedRAMP (Moderato)
- Best practice operative per FFIEC
- Best practice operative per il Cloud Computing Compliance Criteria Catalog (C5) in Germania
- Best practice operative per il Gramm Leach Bliley Act (GLBA)
- Best practice operative per GxP dell'UE Allegato 11
- Best practice operative per la sicurezza HIPAA
- Best practice operative per IRS 1075
- Best practice operative per K-ISMS
- Best practice operative per il bilanciamento del carico
- Best practice operative per la registrazione
- Best practice operative per i servizi di gestione e governance
- Best practice operative per MAS Notice 655
- Best practice operative per MAS TRMG
- Best practice operative per il monitoraggio
- Best practice operative per NBC TRMG
- Best practice operative per NERC CIP BCSI
- Best practice operative per i principi di sicurezza cloud NCSC
- Best practice operative per NCSC Cyber Assessment Framework
- Best practice operative per servizi di rete e distribuzione di contenuti
- Best practice operative per NIST 800-53 rev 4
- Best practice operative per NIST 800-53 rev 5
- Best practice operative per NIST 800 171
- Best practice operative per NIST 800 172
- Best practice operative per NIST 800 181
- Best practice operative per NIST 1800 25

- Best practice operative per NIST CSF
- Best practice operative per NIST Privacy Framework v1.0
- Best practice operative per NYDFS 23
- Best practice operative per NZISM
- Best practice operative per PCI DSS 3.2.1
- Best practice operative per risorse accessibili pubblicamente
- Best practice operative per RBI Cyber Security Framework per UCB
- Best practice operative per RBI MD-ITF
- Best practice operative per servizi di sicurezza, identità e conformità
- Best practice operative per serverless
- Best practice operative per servizi di archiviazione
- Best practice operative per SWIFT CSP
- Best practice di sicurezza per Amazon Elastic Container Service (Amazon ECS)
- Best practice di sicurezza per Amazon Elastic File System (Amazon EFS)
- Best practice di sicurezza per Amazon Elastic Kubernetes Service (Amazon EKS)
- Best practice di sicurezza per Amazon CloudFront
- Best practice di sicurezza per Amazon OpenSearch Service
- Best practice di sicurezza per Amazon Redshift
- Best practice di sicurezza per Amazon Relational Database Service (Amazon RDS)
- Best practice di sicurezza per AWS Auto Scaling
- Best practice di sicurezza per AWS CloudTrail
- Best practice di sicurezza per AWS CodeBuild
- Best practice di sicurezza per Amazon ECR
- Best practice di sicurezza per AWS Lambda
- Best practice di sicurezza per AWS Network Firewall
- Best practice di sicurezza per Amazon SageMaker
- Best practice di sicurezza per AWS Secrets Manager
- Best practice di sicurezza per AWS WAF
- Modelli di esempio con azione di correzione

AWSPacchetto di conformità Control Tower Detective Guardrails

Il modello è disponibile su GitHub: AWSControl Tower Detective Guardrails Conformance Pack.

Best practice operative per ABS CCIG 2.0 Material Workloads

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra la ABS Cloud Computing Implementation Guide 2.0 - Material Workloads e le regole AWS Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli della ABS Cloud Computing Implementation Guide. Un controllo ABS Cloud Computing Implementation Guide può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	AWS Regola di Config	Linea guida
section4a-govern-the-cloud-2-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
section4a-govern-the-cloud-2-material-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
		AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
section4a-govern-the-cloud-2-standard-workloads	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportar e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indiriz zo IP e l'ora dell'evento.

ID controllo	AWS Regola di Config	Linea guida
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
section4a-govern-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4a-govern-the-cloud-2-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
section4a-govern-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4a-govern-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
section4a-govern-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
section4a-govern-the-cloud-3-material-workloads	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCU Threshold Percentage (Config Default: 80) e AccountWCU Threshold Percentage (Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4a-govern-the-cloud-3-material-workloads	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.
section4a-govern-the-cloud-3-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4a-govern-the-cloud-3-standard-workloads	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.
section4a-govern-the-cloud-3-standard-workloads	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'elimina zione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata , potrebbe violare il concetto di funzionalità minima.

ID controllo	AWS Regola di Config	Linea guida
section4a-govern-the-cloud-3-standard-workloads	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
section4a-govern-the-cloud-3-standard-workloads	vpc-network-acl-unused-check	Questa regola garantisc e che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.
section4b-design-and-secure-the-cloud-1-standard-workloads	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-1-standard-workloads	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazioni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
section4b-design-and-secure-the-cloud-1-standard-workloads	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
section4b-design-and-secure-the-cloud-1-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
section4b-design-and-secure-the-cloud-1-standard-workloads	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-nonprivileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
section4b-design-and-secure-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
section4b-design-and-secure-the-cloud-2-standard-workloads	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-3-material-workloads	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
section4b-design-and-secure-the-cloud-3-material-workloads	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-3-material-workloads	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
section4b-design-and-secure-the-cloud-3-material-workloads	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-3-material-workloads	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-3-material-workloads	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
section4b-design-and-secure-the-cloud-3-standard-workloads	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-3-standard-workloads	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
section4b-design-and-secure-the-cloud-3-standard-workloads	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-3-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.
section4b-design-and-secure-the-cloud-4-material-workloads	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
section4b-design-and-secure-the-cloud-4-material-workloads	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-4-material-workloads	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-4-material-workloads	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
section4b-design-and-secure-the-cloud-4-material-workloads	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.
section4b-design-and-secure-the-cloud-4-material-workloads	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
section4b-design-and-secure-the-cloud-4-material-workloads	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-4-material-workloads	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-4-material-workloads	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.
section4b-design-and-secure-the-cloud-4-material-workloads	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-material-workloads	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
section4b-design-and-secure-the-cloud-4-standard-workloads	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
section4b-design-and-secure-the-cloud-4-standard-workloads	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.
section4b-design-and-secure-the-cloud-4-standard-workloads	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazioni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-4-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
section4b-design-and-secure-the-cloud-4-standard-workloads	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
section4b-design-and-secure-the-cloud-4-standard-workloads	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-4-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
section4b-design-and-secure-the-cloud-5-material-workloads	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.
section4b-design-and-secure-the-cloud-5-material-workloads	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-5-material-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
section4b-design-and-secure-the-cloud-5-material-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-5-material-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-5-standard-workloads	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
section4b-design-and-secure-the-cloud-5-standard-workloads	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-5-standard-workloads	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie in Key Management Service (KMS). AWS AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
section4b-design-and-secure-the-cloud-6-material-workloads	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-6-material-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-6-material-workloads	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-6-material-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-6-material-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-6-material-workloads	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che le chiavi master dei clienti (CMK) necessarie non siano pianificate per l'eliminazione nel AWS Key Management Service (KMS).AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
section4b-design-and-secure-the-cloud-6-standard-workloads	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché nell' SageMaker endpoint possono esistere dati sensibili inattivi, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-material-workloads	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4b-design-and-secure-the-cloud-8-material-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-material-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
section4b-design-and-secure-the-cloud-8-material-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-material-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-8-standard-workloads	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
section4b-design-and-secure-the-cloud-8-standard-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazioni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-9-material-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-9-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
section4b-design-and-secure-the-cloud-9-material-workloads	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-9-material-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
section4b-design-and-secure-the-cloud-9-material-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-9-material-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-9-material-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-9-standard-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
section4b-design-and-secure-the-cloud-10-material-workloads	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-10-material-workloads	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-10-material-workloads	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-10-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-10-material-workloads	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4b-design-and-secure-the-cloud-10-material-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
section4b-design-and-secure-the-cloud-10-material-workloads	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
section4b-design-and-secure-the-cloud-10-material-workloads	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
section4b-design-and-secure-the-cloud-10-material-workloads	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
section4b-design-and-secure-the-cloud-10-material-workloads	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-10-material-workloads	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-10-material-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-10-material-workloads	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.
section4b-design-and-secure-the-cloud-10-material-workloads	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-material-workloads	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
section4b-design-and-secure-the-cloud-10-standard-workloads	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza . Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
section4b-design-and-secure-the-cloud-10-standard-workloads	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
section4b-design-and-secure-the-cloud-10-standard-workloads	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
section4b-design-and-secure-the-cloud-10-standard-workloads	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-10-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
section4b-design-and-secure-the-cloud-11-material-workloads	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
section4b-design-and-secure-the-cloud-11-material-workloads	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indiriz zo IP e l'ora dell'evento.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-11-material-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
section4b-design-and-secure-the-cloud-11-material-workloads	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-11-material-workloads	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
section4b-design-and-secure-the-cloud-11-material-workloads	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-11-material-workloads	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
section4b-design-and-secure-the-cloud-11-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-11-material-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.
section4b-design-and-secure-the-cloud-11-material-workloads	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-11-material-workloads	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-11-material-workloads	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-11-material-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
section4b-design-and-secure-the-cloud-11-material-workloads	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-11-material-workloads	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
section4b-design-and-secure-the-cloud-12-standard-workloads	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
section4b-design-and-secure-the-cloud-12-standard-workloads	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
section4b-design-and-secure-the-cloud-12-standard-workloads	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-12-standard-workloads	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
section4b-design-and-secure-the-cloud-12-standard-workloads	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
section4b-design-and-secure-the-cloud-12-standard-workloads	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-12-standard-workloads	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché nell' SageMaker endpoint possono esistere dati sensibili inattivi, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-14-material-workloads	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
section4b-design-and-secure-the-cloud-14-material-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-material-workloads	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.
section4b-design-and-secure-the-cloud-14-material-workloads	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-material-workloads	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.
section4b-design-and-secure-the-cloud-14-material-workloads	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-material-workloads	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
section4b-design-and-secure-the-cloud-14-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-material-workloads	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
section4b-design-and-secure-the-cloud-14-material-workloads	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-material-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
section4b-design-and-secure-the-cloud-14-standard-workloads	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
section4b-design-and-secure-the-cloud-14-standard-workloads	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
section4b-design-and-secure-the-cloud-14-standard-workloads	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
section4b-design-and-secure-the-cloud-14-standard-workloads	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
section4b-design-and-secure-the-cloud-14-standard-workloads	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
section4b-design-and-secure-the-cloud-15-material-workloads	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-15-material-workloads	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
section4b-design-and-secure-the-cloud-15-material-workloads	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-15-material-workloads	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.
section4b-design-and-secure-the-cloud-15-standard-workloads	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.
section4b-design-and-secure-the-cloud-15-standard-workloads	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-15-standard-workloads	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-15-standard-workloads	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-15-standard-workloads	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master dei clienti (CMK) necessarie nel AWS Key Management Service (KMS).AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
section4b-design-and-secure-the-cloud-15-standard-workloads	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	AWS Regola di Config	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
section4c-run-the-cloud-1-standard-workloads	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-2-material-workloads	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
section4c-run-the-cloud-2-material-workloads	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.
section4c-run-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-2-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.
section4c-run-the-cloud-2-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-2-standard-workloads	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4c-run-the-cloud-2-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-2-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
section4c-run-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-3-standard-workloads	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-3-standard-workloads	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-3-standard-workloads	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-3-standard-workloads	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
section4c-run-the-cloud-3-standard-workloads	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-3-standard-workloads	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
section4c-run-the-cloud-3-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-3-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-3-standard-workloads	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
section4c-run-the-cloud-3-standard-workloads	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-3-standard-workloads	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-3-standard-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
section4c-run-the-cloud-3-standard-workloads	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-3-standard-workloads	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
section4c-run-the-cloud-4-standard-workloads	response-plan-exists-maintained (controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti.
section4c-run-the-cloud-4-material-workloads	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-4-material-workloads	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
section4c-run-the-cloud-4-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-4-material-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-5-standard-workloads	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.
section4c-run-the-cloud-5-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-5-standard-workloads	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-5-standard-workloads	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCU Threshold Percentage (Config Default: 80) e AccountWCU Threshold Percentage (Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-5-standard-workloads	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.
section4c-run-the-cloud-5-standard-workloads	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-5-standard-workloads	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-5-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individua re le possibili cause su cui indagare.
section4c-run-the-cloud-6-material-workloads	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-6-material-workloads	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.
section4c-run-the-cloud-6-material-workloads	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-6-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
section4c-run-the-cloud-6-material-workloads	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-6-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
section4c-run-the-cloud-6-standard-workloads	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-6-standard-workloads	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
section4c-run-the-cloud-6-standard-workloads	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for ABS CCIG 2.0 Material Workloads.

Best practice operative per ABS CCIG 2.0 Standard Workloads

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra la ABS Cloud Computing Implementation Guide 2.0 - Carichi di lavoro standard e le regole AWS Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli della ABS Cloud Computing Implementation Guide. Un controllo ABS Cloud Computing Implementation Guide può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	AWS Regola di configurazione	Linea guida
section4a-govern-the-cloud-2-standard-workloads	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportar e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
section4a-govern-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato

ID controllo	AWS Regola di configurazione	Linea guida
		numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.
section4a-govern-the-cloud-2-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di configurazione	Linea guida
section4a-govern-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
section4a-govern-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di configurazione	Linea guida
section4a-govern-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
section4a-govern-the-cloud-3-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
section4a-govern-the-cloud-3-standard-workloads	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.
section4a-govern-the-cloud-3-standard-workloads	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'elimina zione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata , potrebbe violare il concetto di funzionalità minima.

ID controllo	AWS Regola di configurazione	Linea guida
section4a-govern-the-cloud-3-standard-workloads	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
section4a-govern-the-cloud-3-standard-workloads	vpc-network-acl-unused-check	Questa regola garantisc e che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.
section4b-design-and-secure-the-cloud-1-standard-workloads	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-1-standard-workloads	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazioni amministrative su ogni principale.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I

ID controllo	AWS Regola di configurazione	Linea guida
		valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
section4b-design-and-secure-the-cloud-1-standard-workloads	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
section4b-design-and-secure-the-cloud-1-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
section4b-design-and-secure-the-cloud-1-standard-workloads	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-nonprivileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-1-standard-workloads	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
section4b-design-and-secure-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
section4b-design-and-secure-the-cloud-2-standard-workloads	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-3-standard-workloads	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-3-standard-workloads	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
section4b-design-and-secure-the-cloud-3-standard-workloads	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-3-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.
section4b-design-and-secure-the-cloud-4-standard-workloads	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
section4b-design-and-secure-the-cloud-4-standard-workloads	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.
section4b-design-and-secure-the-cloud-4-standard-workloads	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazioni amministrative su ogni principale.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-4-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I

ID controllo	AWS Regola di configurazione	Linea guida
		valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
section4b-design-and-secure-the-cloud-4-standard-workloads	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
section4b-design-and-secure-the-cloud-4-standard-workloads	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-4-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-4-standard-workloads	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
section4b-design-and-secure-the-cloud-5-standard-workloads	acm-certificate-expiration-check	Garantisci la protezion e dell'integrità della rete assicurando che i certifica ti X509 vengano emessi da ACM. AWS Questi certifica ti devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
section4b-design-and-secure-the-cloud-5-standard-workloads	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-5-standard-workloads	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie in Key Management Service (KMS). AWS AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
section4b-design-and-secure-the-cloud-6-standard-workloads	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
section4b-design-and-secure-the-cloud-6-standard-workloads	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.
section4b-design-and-secure-the-cloud-6-standard-workloads	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-6-standard-workloads	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
section4b-design-and-secure-the-cloud-8-standard-workloads	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazioni amministrative su ogni principale.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I

ID controllo	AWS Regola di configurazione	Linea guida
		valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-9-standard-workloads	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-9-standard-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
section4b-design-and-secure-the-cloud-10-standard-workloads	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
section4b-design-and-secure-the-cloud-10-standard-workloads	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
section4b-design-and-secure-the-cloud-10-standard-workloads	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
section4b-design-and-secure-the-cloud-10-standard-workloads	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-10-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-10-standard-workloads	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
section4b-design-and-secure-the-cloud-12-standard-workloads	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
section4b-design-and-secure-the-cloud-12-standard-workloads	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-12-standard-workloads	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
section4b-design-and-secure-the-cloud-12-standard-workloads	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-12-standard-workloads	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
section4b-design-and-secure-the-cloud-12-standard-workloads	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
section4b-design-and-secure-the-cloud-12-standard-workloads	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.
section4b-design-and-secure-the-cloud-12-standard-workloads	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-12-standard-workloads	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-12-standard-workloads	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
section4b-design-and-secure-the-cloud-14-standard-workloads	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
section4b-design-and-secure-the-cloud-14-standard-workloads	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
section4b-design-and-secure-the-cloud-14-standard-workloads	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
section4b-design-and-secure-the-cloud-14-standard-workloads	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
section4b-design-and-secure-the-cloud-14-standard-workloads	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-14-standard-workloads	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
section4b-design-and-secure-the-cloud-14-standard-workloads	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.
section4b-design-and-secure-the-cloud-15-standard-workloads	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-15-standard-workloads	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-15-standard-workloads	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-15-standard-workloads	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
section4b-design-and-secure-the-cloud-15-standard-workloads	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che le chiavi master del cliente (CMK) necessarie non siano pianificate per l'eliminazione in AWS Key Management Service (KMS).AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
section4b-design-and-secure-the-cloud-15-standard-workloads	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
section4c-run-the-cloud-1-standard-workloads	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.
section4c-run-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-2-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.
section4c-run-the-cloud-2-standard-workloads	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-2-standard-workloads	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
section4c-run-the-cloud-2-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-2-standard-workloads	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
section4c-run-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-3-standard-workloads	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-3-standard-workloads	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-3-standard-workloads	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-3-standard-workloads	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
section4c-run-the-cloud-3-standard-workloads	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-3-standard-workloads	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
section4c-run-the-cloud-3-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-3-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-3-standard-workloads	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
section4c-run-the-cloud-3-standard-workloads	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-3-standard-workloads	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-3-standard-workloads	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-3-standard-workloads	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
section4c-run-the-cloud-3-standard-workloads	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-3-standard-workloads	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
section4c-run-the-cloud-3-standard-workloads	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.
section4c-run-the-cloud-4-standard-workloads	response-plan-exists-maintained (controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-5-standard-workloads	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.
section4c-run-the-cloud-5-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-5-standard-workloads	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-5-standard-workloads	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCU Threshold Percentage (Config Default: 80) e AccountWCU Threshold Percentage (Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-5-standard-workloads	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.
section4c-run-the-cloud-5-standard-workloads	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-5-standard-workloads	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-5-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individua re le possibili cause su cui indagare.
section4c-run-the-cloud-6-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-6-standard-workloads	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
section4c-run-the-cloud-6-standard-workloads	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
section4c-run-the-cloud-6-standard-workloads	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for ABS CCIG 2.0 Standard Workloads.

Best practice operative per ACSC Essentials 8

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il modello Essential Eight Maturity dell'Australian Cyber Security Centre (ACSC) e le regole di Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli ACSC Essential Eight. Un controllo CSC Essential Eight può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature. Alcune delle mappature utilizzate nelle regole di configurazione si riferiscono alla sezione di ordine superiore (ad es. Strategie di mitigazione per limitare l'entità degli incidenti di sicurezza informatica) rispetto alle sezioni più prescrittive.

Questo modello di pacchetto di conformità di esempio contiene le mappature dei controlli all'interno di ACSC Essential 8, creato dal Commonwealth australiano e disponibile all'indirizzo ACSC | Essential

Eight. La licenza del framework ai sensi del Creative Commons Attribution 4.0 International Public License e le informazioni sul diritto d'autore del framework (inclusa una clausola di esclusione delle responsabilità) sono disponibili all'indirizzo ACSC | Copyright.

ID controllo	AWS Regola di Config	Linea guida
Application_control	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
Application_control	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
Application_control	ec2-instance-managed-by-sys tems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione

ID controllo	AWS Regola di Config	Linea guida
		è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
Application_control	waf-regional-rule-not-empty	Assicurati che il tuo AWS WAF abbia una regola che non sia vuota. Una regola senza condizioni può comportare un comportamento non intenzion ale.
Application_control	waf-regional-rulegroup-not-empty	Assicurati che il tuo AWS WAF abbia un gruppo di regole che non sia vuoto. Un gruppo di regole vuoto potrebbe causare un comportamento indesider ato.

ID controllo	AWS Regola di Config	Linea guida
Application_control	waf-regional-webacl-not-empty	Un ACL Web allegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.
Application_control	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
Patch_applications	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per protegger e l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
Patch_applications	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
Patch_applications	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribui ti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.
Patch_applications	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornam enti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornamenti, correzion i e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	AWS Regola di Config	Linea guida
Patch_applications	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.
Patch_applications	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
Patch_applications	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
Restrict_administrative_privileges	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
Restrict_administrative_privileges	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
Restrict_administrative_privileges	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
Restrict_administrative_privileges	codebuild-project-environment-privileged-check	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che il tuo ambiente di CodeBuild progetto Amazon non abbia la modalità privilegiata abilitata. Questa impostazione deve essere disabilitata per impedire l'accesso involontario alle API Docker e all'hardware sottostante del container.

ID controllo	AWS Regola di Config	Linea guida
Restrict_administrative_privileges	ecs-containers-nonprivileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).
Restrict_administrative_privileges	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
Restrict_administrative_privileges	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).

ID controllo	AWS Regola di Config	Linea guida
Restrict_administrative_privileges	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.
Restrict_administrative_privileges	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
Restrict_administrative_privileges	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
Restrict_administrative_privileges	rds-instance-iam-authentication-enabled	Assicurati che l'autenticazione AWS Identity and Access Management (IAM) sia abilitata sulle istanze di Amazon Relational Database Service (Amazon RDS) per controllare l'accesso a sistemi e asset. In questo modo il traffico di rete da e verso il database viene crittografato utilizzando Secure Sockets Layer (SSL). Non devi archiviare le credenziali dell'utente nel database, perché l'autenticazione è gestita esternamente.
Restrict_administrative_privileges	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
Restrict_administrative_privileges	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	AWS Regola di Config	Linea guida
Restrict_administrative_privileges	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
Restrict_administrative_privileges	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.
Restrict_administrative_privileges	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
Patch_operating_systems	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
Multi-factor_authentication	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
Multi-factor_authentication	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richieden do l'autenticazione a più fattori per gli utenti.
Multi-factor_authentication	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
Multi-factor_authentication	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
Multi-factor_authentication	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
Regular_backups	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
Regular_backups	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
Regular_backups	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
Regular_backups	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
Regular_backups	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.
Regular_backups	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
Regular_backups	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
Regular_backups	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.

ID controllo	AWS Regola di Config	Linea guida
Regular_backups	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
Regular_backups	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfar e i requisiti di conformit à aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyV alue (Config default: 1), (requiredRetentionD aysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
Regular_backups	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.
Regular_backups	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
Regular_backups	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for ACSC Essential 8.

Best practice operative per ACSC ISM

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra l'Australian Cyber Security Centre (ACSC) Information Security Manual (ISM) 2020-06 e le regole di Config gestite. AWS Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli ISM. Un controllo ISM può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo modello di pacchetto di conformità di esempio contiene le mappature dei controlli all'interno del framework ISM, creato dal Commonwealth australiano e disponibile nell'Australian Government Information Security Manual. La licenza del framework ai sensi del Creative Commons Attribution 4.0 International Public License e le informazioni sul diritto d'autore del framework (inclusa una clausola di esclusione delle responsabilità) sono disponibili all'indirizzo ACSC | Copyright.

ID controllo	AWS Regola di Config	Linea guida
43	response-plan-exists-maintained (controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti.
252	security-awareness-program-exists (controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.
261	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
261	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente.

ID controllo	AWS Regola di Config	Linea guida
		Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
261	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di Config	Linea guida
298	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
298	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
298	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
298	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	AWS Regola di Config	Linea guida
380	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizza zioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.
459	api-gw-cache-enabled-and-en crypted	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
459	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di Config	Linea guida
459	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
459	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
459	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
459	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
459	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
459	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
459	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
459	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	AWS Regola di Config	Linea guida
459	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
459	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
459	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
459	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.
459	codebuild-project-s3-logs-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per AWS CodeBuild i log archiviati in Amazon S3.
459	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
459	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	AWS Regola di Config	Linea guida
459	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
459	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
459	sns-encrypted-kms	Per proteggere i dati archiviat i, assicurati che gli argomenti di Amazon Simple Notificat ion Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittogra fia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
580	audit-log-policy-exists (controllo del processo)	Definizione e mantenimento di una policy di gestione dei log di audit che definisca i requisiti di gestione dei log dell'organizzazione. Ciò include, a titolo esemplificativo, la revisione e la conservazione dei log di audit.
634	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
859	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	AWS Regola di Config	Linea guida
974	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richieden do l'autenticazione a più fattori per gli utenti.
974	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
1139	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB SecurityPolicy -TLS-1-2-2017-0. Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1173	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
1173	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
1173	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
1173	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richieden do l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
1173	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
1228	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
1240	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
1240	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	AWS Regola di Config	Linea guida
1271	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
1271	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
1277	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
1277	rds-instance-iam-authentication-enabled	Assicurati che l'autenticazione AWS Identity and Access Management (IAM) sia abilitata sulle istanze di Amazon Relational Database Service (Amazon RDS) per controllare l'accesso a sistemi e asset. In questo modo il traffico di rete da e verso il database viene crittografato utilizzando Secure Sockets Layer (SSL). Non devi archiviare le credenziali dell'utente nel database, perché l'autenticazione è gestita esternamente.
1277	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	AWS Regola di Config	Linea guida
1380	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per protegger e l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
1380	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
1380	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribui ti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.
1380	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornam enti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornamenti, correzion i e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	AWS Regola di Config	Linea guida
1380	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.
1380	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
1380	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1380	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.
1380	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
1380	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
1380	codebuild-project-environment-privileged-check	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che il tuo ambiente di CodeBuild progetto Amazon non abbia la modalità privilegiata abilitata. Questa impostazione deve essere disabilitata per impedire l'accesso involontario alle API Docker e all'hardware sottostante del container.

ID controllo	AWS Regola di Config	Linea guida
1380	ecs-containers-nonprivileged	Per facilitare l'impleme ntazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).
1380	ecs-containers-readonly-acc ess	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizza zioni esplicite di lettura/s crittura.
1380	ecs-task-definition-nonroot-user	Per facilitare l'impleme ntazione del principio del privilegio minimo, assicurat i che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).

ID controllo	AWS Regola di Config	Linea guida
1380	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.
1380	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
1380	rds-instance-iam-authentication-enabled	Assicurati che l'autenticazione AWS Identity and Access Management (IAM) sia abilitata sulle istanze di Amazon Relational Database Service (Amazon RDS) per controllare l'accesso a sistemi e asset. In questo modo il traffico di rete da e verso il database viene crittografato utilizzando Secure Sockets Layer (SSL). Non devi archiviare le credenziali dell'utente nel database, perché l'autenticazione è gestita esternamente.
1380	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
1380	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	AWS Regola di Config	Linea guida
1380	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1380	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.
1380	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
1388	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1388	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
1401	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
1401	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richieden do l'autenticazione a più fattori per gli utenti.
1401	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
1401	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
1401	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
1402	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
1404	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.
1405	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatc h per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusi one dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
1405	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
1405	multi-region-cloudtrail-enabled	MULTI_REGION_CLOUD_TRAIL_ENABLED
1405	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	AWS Regola di Config	Linea guida
1405	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
1405	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
1405	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	AWS Regola di Config	Linea guida
1405	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
1405	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1405	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
1405	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
1405	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
1405	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di Config	Linea guida
1405	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.
1405	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.
1405	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	AWS Regola di Config	Linea guida
1405	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
1490	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di Config	Linea guida
1490	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
1490	waf-regional-rule-not-empty	Assicurati che il tuo AWS WAF abbia una regola che non sia vuota. Una regola senza condizioni può comportare un comportamento non intenzion ale.
1490	waf-regional-rulegroup-not-empty	Assicurati che il tuo AWS WAF abbia un gruppo di regole che non sia vuoto. Un gruppo di regole vuoto potrebbe causare un comportamento indesider ato.

ID controllo	AWS Regola di Config	Linea guida
1490	waf-regional-webacl-not-empty	Un ACL Web collegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.
1490	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
1501	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
1504	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
1504	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richieden do l'autenticazione a più fattori per gli utenti.
1504	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
1504	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
1504	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
1509	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
1509	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di Config	Linea guida
1509	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.
1509	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrai l, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittogra fia dei log, la convalida dei log e l'abilitazione AWS CloudTrai l in più aree.

ID controllo	AWS Regola di Config	Linea guida
1509	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
1509	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
1509	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	AWS Regola di Config	Linea guida
1509	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
1509	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1509	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
1509	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
1509	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
1509	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di Config	Linea guida
1509	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.
1509	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.
1509	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	AWS Regola di Config	Linea guida
1509	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
1511	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	AWS Regola di Config	Linea guida
1511	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
1511	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	AWS Regola di Config	Linea guida
1511	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
1511	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
1511	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.
1511	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
1511	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.
1511	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	AWS Regola di Config	Linea guida
1511	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
1511	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfar e i requisiti di conformit à aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyV alue (Config default: 1), (requiredRetentionD aysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1511	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1511	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
1511	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
1511	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	AWS Regola di Config	Linea guida
1511	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfar e i requisiti di conformit à aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyV alue (Config default: 1), (requiredRetentionD aysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1511	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.
1515	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	AWS Regola di Config	Linea guida
1515	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
1515	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
1515	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
1515	elasticache-redis-cluster-a utomatic-backup-check	Quando i backup automatic i sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornalie ra. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazion e. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	AWS Regola di Config	Linea guida
1515	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
1515	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	AWS Regola di Config	Linea guida
1515	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.
1515	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
1515	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfar e i requisiti di conformit à aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyV alue (Config default: 1), (requiredRetentionD aysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1515	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.
1515	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
1515	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.
1536	cloudtrail-s3-dataevents-en abled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indiriz zo IP e l'ora dell'evento.

ID controllo	AWS Regola di Config	Linea guida
1537	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
1537	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1552	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
1552	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
1552	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Regola di Config	Linea guida
1552	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
1552	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
1579	dynamodb-autoscaling-enable d	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	AWS Regola di Config	Linea guida
1580	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di Config	Linea guida
1580	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di Config	Linea guida
1580	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relational Database Service (Amazon RDS). Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.
1650	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
1650	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di Config	Linea guida
1650	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.
1650	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrai l, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittogra fia dei log, la convalida dei log e l'abilitazione AWS CloudTrai l in più aree.

ID controllo	AWS Regola di Config	Linea guida
1650	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
1650	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
1650	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	AWS Regola di Config	Linea guida
1650	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
1650	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1650	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
1650	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
1650	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
1650	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di Config	Linea guida
1650	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.
1650	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.
1650	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	AWS Regola di Config	Linea guida
1650	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
1657	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di Config	Linea guida
1657	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
1657	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
1657	waf-regional-rule-not-empty	Assicurati che il tuo AWS WAF abbia una regola che non sia vuota. Una regola senza condizioni può comportare un comportamento non intenzion ale.
1657	waf-regional-rulegroup-not-empty	Assicurati che il tuo AWS WAF abbia un gruppo di regole che non sia vuoto. Un gruppo di regole vuoto potrebbe causare un comportamento indesider ato.
1657	waf-regional-webacl-not-empty	Un ACL Web collegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.

ID controllo	AWS Regola di Config	Linea guida
1657	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.
1661	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
1661	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di Config	Linea guida
1661	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.
1661	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrai l, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittogra fia dei log, la convalida dei log e l'abilitazione AWS CloudTrai l in più aree.

ID controllo	AWS Regola di Config	Linea guida
1661	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
1661	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
1661	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	AWS Regola di Config	Linea guida
1661	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
1661	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1661	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
1661	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
1661	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
1661	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di Config	Linea guida
1661	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
1679	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
1679	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richieden do l'autenticazione a più fattori per gli utenti.
1679	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
1679	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
1679	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
1680	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
1680	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richieden do l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
1680	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
1680	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
1680	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
1681	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
1681	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richieden do l'autenticazione a più fattori per gli utenti.
1681	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
1681	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
1681	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
1683	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
1683	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di Config	Linea guida
1690	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per protegger e l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
1690	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
1690	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribui ti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.
1690	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornam enti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornamenti, correzion i e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	AWS Regola di Config	Linea guida
1690	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.
1690	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
1690	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1691	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per protegger e l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
1691	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
1691	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribui ti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.
1691	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornam enti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornamenti, correzion i e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	AWS Regola di Config	Linea guida
1691	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.
1691	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
1691	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1693	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per protegger e l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
1693	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
1693	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribui ti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.
1693	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornam enti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornamenti, correzion i e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	AWS Regola di Config	Linea guida
1693	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.
1693	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
1693	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.
1694	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
1695	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
1707	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.

ID controllo	AWS Regola di Config	Linea guida
P1	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
P1	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di Config	Linea guida
P3	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per protegger e l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
P5	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
P7	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
P7	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
P7	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
P7	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	AWS Regola di Config	Linea guida
P8	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di Config	Linea guida
P9	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
P9	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfar e i requisiti di conformit à aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyV alue (Config default: 1), (requiredRetentionD aysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.
P9	backup-recovery-point-encrypted	Assicurati che la crittogra fia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
P9	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.
P9	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
P9	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
P9	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
P9	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
P9	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
P9	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
P9	elasticache-redis-cluster-a utomatic-backup-check	Quando i backup automatic i sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornalie ra. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazion e. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	AWS Regola di Config	Linea guida
P9	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
P9	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
P9	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.
P10	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
P10	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.

ID controllo	AWS Regola di Config	Linea guida
P10	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
P10	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.
P10	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
P11	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for ACSC ISM.

Best practice operative per IA e ML

Questo pacchetto di conformità contiene AWS Config regole basate su AI e ML. Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for AI e ML.

Best practice operative per Gateway Amazon API

Questo pacchetto di conformità contiene AWS Config regole basate sull'utilizzo di Amazon API Gateway all'interno. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, consulta Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Amazon API Gateway.

Best practice operative per Amazon CloudWatch

Questo pacchetto di conformità contiene AWS Config regole basate sull'utilizzo di Amazon CloudWatch Within. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, consulta Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Amazon CloudWatch.

Best practice operative per Amazon DynamoDB

Il modello è disponibile su GitHub: Operational Best Practices for Amazon DynamoDB.

Best practice operative per Amazon S3

Il modello è disponibile su GitHub: Operational Best Practices for Amazon S3.

Best practice operative per APRA CPG 234

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra l'Australian Prudential Regulation Authority (APRA) CPG 234 e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli APRA CPG 234. Un controllo APRA CPG 234 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo modello di pacchetto di conformità di esempio contiene le mappature dei controlli all'interno dell'APRA CPG 234 2019, creato dal Commonwealth australiano e disponibile nella Prudential Practice Guide: CPG 234 Information Security. La licenza del framework ai sensi del Creative Commons Australia Attribution 3.0 Licence e le informazioni sul diritto d'autore del framework (inclusa una clausola di esclusione delle responsabilità) sono disponibili all'indirizzo APRA | Copyright.

ID controllo	AWS Regola di Config	Linea guida
36a	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
36a	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.
36a	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e

ID controllo	AWS Regola di Config	Linea guida
		la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
36b	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
36b	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.
36b	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
36b	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
36b	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
36b	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
36b	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	AWS Regola di Config	Linea guida
36c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
36c	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
36c	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.

ID controllo	AWS Regola di Config	Linea guida
36c	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
36c	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
36c	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
36c	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.
36c	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
36c	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	AWS Regola di Config	Linea guida
36d	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
36d	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
36d	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
36d	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
36d	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
36d	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
36d	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
36d	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
36d	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
36d	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
36d	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
36d	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
36d	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
36d	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
36d	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
36d	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
36d	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
36d	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
36d	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
36d	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
36d	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
36d	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richieden do l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
36d	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibili tà che un'identità riceva o mantenga privilegi eccessivi.
36d	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	AWS Regola di Config	Linea guida
36d	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
36d	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
36d	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
36d	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per protegger e l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	AWS Regola di Config	Linea guida
36d	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.

ID controllo	AWS Regola di Config	Linea guida
36d	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
36d	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.
36d	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associa zione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
36d	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
36d	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.
36d	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
36d	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
36d	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	AWS Regola di Config	Linea guida
36d	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
36d	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	AWS Regola di Config	Linea guida
36d	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
36d	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	AWS Regola di Config	Linea guida
36d	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
36e	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	AWS Regola di Config	Linea guida
36e	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
36e	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
36e	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
36e	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
36e	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di Config	Linea guida
36e	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.
36e	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
36e	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
36e	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
36e	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
36e	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
36e	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
36e	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
36e	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
36e	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
36e	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
36e	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associa zione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.
36e	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
36e	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
36e	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
36e	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicam ente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di Config	Linea guida
36e	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
36e	api-gw-associated-with-waf	AWS WAF ti consente di configurare una serie di regole (chiamate lista di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personali zzabili da te definite. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	AWS Regola di Config	Linea guida
36e	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
36e	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	AWS Regola di Config	Linea guida
36e	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
36f	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
36f	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
36f	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
36f	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
36f	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
36f	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
36f	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
36f	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
36f	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
36f	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
36f	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
36f	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
36f	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
36f	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
36f	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
36f	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
36f	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
36f	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS
36f	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di Config	Linea guida
36f	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
36f	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
36f	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
36f	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
36f	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicam ente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di Config	Linea guida
36f	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
36f	api-gw-associated-with-waf	AWS WAF ti consente di configurare una serie di regole (chiamate lista di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personali zzabili da te definite. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	AWS Regola di Config	Linea guida
36f	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
36f	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	AWS Regola di Config	Linea guida
36f	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
36g	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
36g	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
36g	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
36h	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
36h	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
36h	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.
36h	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
36h	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.
36h	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
36h	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
36h	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
36i	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	AWS Regola di Config	Linea guida
36i	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
36i	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCU Threshold Percentage (Config Default: 80) e AccountWCU Threshold Percentage (Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
36i	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
36i	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultane ità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.
36i	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notificat ion Service (Amazon SNS) quando una funzione restituis ce un errore.

ID controllo	AWS Regola di Config	Linea guida
36i	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.
36i	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	AWS Regola di Config	Linea guida
36i	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
36i	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individua re le possibili cause su cui indagare.

ID controllo	AWS Regola di Config	Linea guida
36i	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
36j	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
36j	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
36j	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
36j	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
36j	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	AWS Regola di Config	Linea guida
36j	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
36j	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCU Threshold Percentage (Config Default: 80) e AccountWCU Threshold Percentage (Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
36j	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notificat ion Service (Amazon SNS) quando una funzione restituis ce un errore.
36j	rds-enhanced-monitoring-ena bled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostan te, Enhanced Monitorin g raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondari o e le metriche dell'host secondario.

ID controllo	AWS Regola di Config	Linea guida
36j	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individua re le possibili cause su cui indagare.
36j	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di Config	Linea guida
36l	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
36l	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	AWS Regola di Config	Linea guida
36l	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
36l	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	AWS Regola di Config	Linea guida
36l	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di Config	Linea guida
36l	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di Config	Linea guida
36l	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
36l	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	AWS Regola di Config	Linea guida
36l	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
36l	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
36l	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
36l	elb-cross-zone-load-balanci ng-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalen ti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di Config	Linea guida
36l	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
36l	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
36l	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.
36l	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individua re le possibili cause su cui indagare.

ID controllo	AWS Regola di Config	Linea guida
39(a)(b)(d)	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
39(a)(b)(d)	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
39(a)(b)(d)	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
40	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
40	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
40	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
40	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	AWS Regola di Config	Linea guida
44a	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
44a	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
44a	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
44b	rds-instance-deletion-prote ction-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzion almente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di Config	Linea guida
44b	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.
44b	elb-deletion-protection-ena bled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzion almente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di Config	Linea guida
44c	kms-cmk-not-scheduled-for-deletion	Per contribuire a proteggere i dati archiviati, assicuratevi che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (KMS).AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
44c	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
44c	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
44c	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
45	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
45	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
45	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
45	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richieden do l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
45	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibili tà che un'identità riceva o mantenga privilegi eccessivi.
45	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	AWS Regola di Config	Linea guida
45	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
45	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
45	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
45	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
45	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.
45	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicam ente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
45	ebs-snapshot-public-restora ble-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
45	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
45	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di Config	Linea guida
45	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.
45	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
45	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
45	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
45	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
45	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
45	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
45	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
45	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
45	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.
45	s3-bucket-public-read-prohi bited	Gestisci l'accesso alle risorse nel AWS cloud permetten do solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Regola di Config	Linea guida
45	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
45	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
45	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di Config	Linea guida
45	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
45	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	AWS Regola di Config	Linea guida
45	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
45	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.
45	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associa zione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
45	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
45	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
45	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
45	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
45	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicam ente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di Config	Linea guida
45	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
45	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di Config	Linea guida
45	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
45	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	AWS Regola di Config	Linea guida
47c	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
47c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
47c	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
47c	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
47c	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibili tà che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di Config	Linea guida
47c	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.
47c	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
52c	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	AWS Regola di Config	Linea guida
52c	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
52c	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
52c	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
52c	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
52c	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di Config	Linea guida
52c	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
52c	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
52c	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
52c	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
52c	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
52c	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
52c	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
52c	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	AWS Regola di Config	Linea guida
52c	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
52c	s3-default-encryption-kms	Assicurati che la crittogra fia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittogra fia a riposo per proteggere tali dati.
52c	redshift-cluster-kms-enabled	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
52c	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
52d	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
52d	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Regola di Config	Linea guida
52d	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
52d	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
52d	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
52d	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
52d	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di Config	Linea guida
52d	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.
52d	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
52d	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
52d	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
52d	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
52d	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
52d	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
52d	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
52d	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
52d	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	AWS Regola di Config	Linea guida
52d	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
52d	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	AWS Regola di Config	Linea guida
52d	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
52d	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
52d	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di Config	Linea guida
52d	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
52e	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
52e	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
53	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
53	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Regola di Config	Linea guida
53	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
53	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
53	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
53	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
53	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
53	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
53	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
53	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
53	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
53	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
53	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
53	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
53	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
53	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
53	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
53	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
53	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
53	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicam ente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di Config	Linea guida
53	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	AWS Regola di Config	Linea guida
53	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
53	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	AWS Regola di Config	Linea guida
54	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
54	acm-certificate-expiration-check	Assicurati che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
54	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittogra fate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
54	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
54	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
54	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
54	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	AWS Regola di Config	Linea guida
54	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
54	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
54	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di Config	Linea guida
54	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
54	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
54	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
54	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
54	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
54	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
54	sagemaker-endpoint-configur ation-kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
54	sagemaker-notebook-instance -kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
54	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
54	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
54	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
54	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
54	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
54	redshift-cluster-kms-enabled	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
54	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentir e ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
54	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
55	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
55	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
6.7	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
67	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
67	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
67	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	AWS Regola di Config	Linea guida
67	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di Config	Linea guida
67	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
67	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
67	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
67	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
67	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di Config	Linea guida
67	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.
67	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
67	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
67	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	AWS Regola di Config	Linea guida
67	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
67	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
67	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.
67	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di Config	Linea guida
68	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
68	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
73	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
73	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(b)(h)	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(b)(h)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
AllegatoA_1(b)(h)	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(b)(h)	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
AllegatoA_1(b)(h)	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(b)(h)	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(b)(h)	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(b)(h)	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.
AllegatoA_1(b)(h)	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(b)(h)	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associa zione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.
AllegatoA_1(c)	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(c)	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
AllegatoA_1(e)	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(e)	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
AllegatoA_1(e)	cloudwatch-alarm-action-che ck	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActi onRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(e)	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AllegatoA_1(e)	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
AllegatoA_1(e)	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(e)	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AllegatoA_1(e)	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(e)	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(e)	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
AllegatoA_1(e)	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(e)	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
AllegatoA_1(e)	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di Config	Linea guida
AllegatoA_1(e)	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
AllegatoA_1(e)	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	AWS Regola di Config	Linea guida
AllegatoB_1	security-awareness-program-exists (controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.
AllegatoC_4	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_4	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_4	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
AllegatoC_4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
AllegatoC_4	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_4	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AllegatoC_4	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_4	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibili tà che un'identità riceva o mantenga privilegi eccessivi.
AllegatoC_4	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_4	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
AllegatoC_4	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_4	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
AllegatoC_4	secretsmanager-rotation-ena bled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianifica zione regolare può abbreviar e il periodo di attività di un segreto e ridurre potenzial mente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_4	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
AllegatoC_4	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_4	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_4	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.
AllegatoC_4	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associa zione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_4	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AllegatoC_5	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_5	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
AllegatoC_5	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_5	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibili tà che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_5	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
AllegatoC_6	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
AllegatoC_6	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_6	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
AllegatoC_7(c)	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_7(h)	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AllegatoC_7(h)	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
AllegatoC_7(h)	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_7(h)	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AllegatoC_7(h)	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_7(h)	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
AllegatoC_7(h)	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_7(h)	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_7(h)	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_7(h)	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
AllegatoC_7(h)	vpc-flow-logs-enabled	I log di flusso VPC forniscon o record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_7(h)	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
AllegatoC_7(h)	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_7(h)	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'inter no dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AllegatoC_7(h)	elasticsearch-logs-to-cloud watch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_7(i)	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.
AllegatoC_7(j)	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richieden do l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_7(j)	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
AllegatoC_7(j)	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_7(j)	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
AllegatoC_8	opensearch-logs-to-cloudwat ch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_8	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AllegatoC_8	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
AllegatoC_8	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_8	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AllegatoC_8	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_8	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_8	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
AllegatoC_8	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_8	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
AllegatoC_8	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di Config	Linea guida
AllegatoC_8	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
AllegatoD_1	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	AWS Regola di Config	Linea guida
AllegatoD_1	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub
AllegatoE_4	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel Key Management Service (KMS). AWS AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
AllegatoE_4	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	AWS Regola di Config	Linea guida
AllegatoE_5(d)	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.
AllegatoE_1(a)(b)(d)	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
AllegatoE_1(a)(b)(d)	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
AllegatoE_1(a)(b)(d)	acm-certificate-expiration-check	Garantisci la protezion e dell'integrità della rete assicurando che i certifica ti X509 vengano emessi da ACM. AWS Questi certifica ti devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
AllegatoE_1(a)(b)(d)	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittogra fate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
AllegatoE_1(a)(b)(d)	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	AWS Regola di Config	Linea guida
AllegatoE_1(a)(b)(d)	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
AllegatoE_1(a)(b)(d)	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
AllegatoE_1(a)(b)(d)	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
AllegatoE_1(a)(b)(d)	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	AWS Regola di Config	Linea guida
AllegatoE_1(a)(b)(d)	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
AllegatoE_1(a)(b)(d)	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
AllegatoE_1(a)(b)(d)	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (KMS).AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	AWS Regola di Config	Linea guida
AllegatoE_1(a)(b)(d)	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
AllegatoE_1(a)(b)(d)	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
AllegatoE_1(a)(b)(d)	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AllegatoE_1(a)(b)(d)	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.
AllegatoE_1(a)(b)(d)	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
AllegatoE_1(a)(b)(d)	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
AllegatoE_1(a)(b)(d)	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
AllegatoE_1(a)(b)(d)	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
AllegatoE_1(a)(b)(d)	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
AllegatoE_1(a)(b)(d)	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
AllegatoE_1(a)(b)(d)	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AllegatoE_1(a)(b)(d)	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AllegatoE_1(a)(b)(d)	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
AllegatoE_1(a)(b)(d)	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentir e ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for APRA CPG 234.

Best practice operative per la gestione degli asset

Questo pacchetto di conformità contiene al suo interno AWS Config regole basate sulla gestione delle risorse. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Asset Management.

Best practice operative per AWS Backup

Questo pacchetto di conformità contiene AWS Config regole basate sull' AWS Backup interno. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for AWS Backup.

Best practice operative per la gestione delle AWS identità e degli accessi

Il modello è disponibile su GitHub: Best practice operative per la gestione delle AWS identità e degli accessi.

Best practice operative per AWS Well-Architected Framework Reliability Pillar

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra Well-Architected Framework Reliability Pillar di Amazon Web Services e le regole di Config gestite. AWS Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più principi di progettazione del pilastro. Una categoria del framework Well-Architected può essere correlata a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-1	Come si gestiscono quote e restrizioni dei servizi? Per le architetture di carichi di lavoro basate sul cloud, esistono quote di servizio (chiamate anche restrizioni dei servizi). Queste quote sono presenti per evitare di effettuare accidentalmente il provisioning di più risorse di quelle necessarie e limitare i tassi di richiesta sulle operazioni API in modo da protegger	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e i servizi da un uso illecito. Esistono anche vincoli di risorse, ad esempio la velocità con cui è possibile trasferire i bit su un cavo in fibra ottica o lo spazio di archiviazione su un disco fisico.		regola genera un avviso quando la velocità di trasmissi one effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltati vamente i parametri AccountRCU ThresholdPercentag e (Config Default: 80) e AccountWCU ThresholdPercentage (Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-1	Come si gestiscon o quote e restrizio ni dei servizi? Per le architetture di carichi di lavoro basate sul cloud, esistono quote di servizio (chiamate anche restrizioni dei servizi). Queste quote sono presenti per evitare di effettuar e accidentalmente il provisioning di più risorse di quelle necessarie e limitare i tassi di richiesta sulle operazioni API in modo da protegger e i servizi da un uso illecito. Esistono anche vincoli di risorse, ad esempio la velocità con cui è possibile trasferire i bit su un cavo in fibra ottica o lo spazio di archiviazione su un disco fisico.	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-1	Come si gestiscon o quote e restrizio ni dei servizi? Per le architetture di carichi di lavoro basate sul cloud, esistono quote di servizio (chiamate anche restrizioni dei servizi). Queste quote sono presenti per evitare di effettuar e accidentalmente il provisioning di più risorse di quelle necessarie e limitare i tassi di richiesta sulle operazioni API in modo da protegger e i servizi da un uso illecito. Esistono anche vincoli di risorse, ad esempio la velocità con cui è possibile trasferire i bit su un cavo in fibra ottica o lo spazio di archiviazione su un disco fisico.	ecs-task-definition-memory-hard-limit	La limitazione della memoria massima disponibile per i container Amazon Elastic Container Service (ECS) garantisce che l'utilizz o delle risorse non possa essere abusato in caso di accesso malevolo ai container.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-2	Come si pianifica la topologia della rete? I carichi di lavoro sono spesso presenti in più ambienti. Questi includono più ambienti cloud (sia accessibili pubblicamente sia privati) e, possibilmente, l'infrastruttura del data center esistente. I piani devono includere considerazioni di rete, ad esempio connettività intrasistema e intersistema, gestione di indirizzi IP pubblici, gestione di indirizzi IP privati e risoluzione dei nomi di dominio.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-2	Come si pianifica la topologia della rete? I carichi di lavoro sono spesso presenti in più ambienti. Questi includono più ambienti cloud (sia accessibili pubblicam ente sia privati) e, possibilmente, l'infrast ruttura del data center esistente. I piani devono includere considerazioni di rete, ad esempio connettiv ità intrasistema e intersistema, gestione di indirizzi IP pubblici, gestione di indirizzi IP privati e risoluzione dei nomi di dominio.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-2	Come si pianifica la topologia della rete? I carichi di lavoro sono spesso presenti in più ambienti. Questi includono più ambienti cloud (sia accessibili pubblicamente sia privati) e, possibilmente, l'infrastruttura del data center esistente. I piani devono includere considerazioni di rete, ad esempio connettività intrasistema e intersistema, gestione di indirizzi IP pubblici, gestione di indirizzi IP privati e risoluzione dei nomi di dominio.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il AWS traffico rimane in modo sicuro all'interno del Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-5	Come si progettan o le interazioni in un sistema distribuito per mitigare o affrontar e gli errori? I sistemi distribuiti si basano sulle reti di comunicaz ione per interconn ettere i component i, ad esempio server o servizi. Il carico di lavoro deve funzionar e in modo affidabil e nonostante la perdita o la latenza dei dati su queste reti. I componenti del sistema distribui to devono funzionar e in modo da non influire negativamente su altri component i o sul carico di lavoro. Queste best practice consenton o di prevenire gli errori e migliorare il tempo medio tra guasti (MTBF).	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	api-gw-xray-enabled	AWS X-Ray raccoglie dati sulle richieste servite dall'appl icazione e fornisce strumenti che è possibile utilizzar e per visualizzare, filtrare e acquisire informazioni su tali dati per identificare problemi e opportuni tà di ottimizzazione. Assicurati che X-Ray sia abilitato in modo da poter visualizzare informazi oni dettagliate non solo sulla richiesta e sulla risposta, ma anche sulle chiamate effettuate dall'appl icazione a AWS risorse downstream, microservizi, database e API Web HTTP.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	api-gw-execution-l ogging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitorano le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazioni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verificano eventi significativi. Il monitoraggio permette al carico di lavoro di riconoscere quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearc h di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservaz ione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibi lità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearc h di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearc h I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosti care problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	ecs-container-insi ghts-enabled	Il monitoraggio è una parte importante per mantenere l'affidab ilità, la disponibi lità e le prestazioni di Amazon Elastic Container Service (ECS) e delle tue AWS soluzioni. Container Insights fornisce inoltre informazioni diagnosti che, ad esempio errori di riavvio del container , che consentono di isolare i problemi e risolverli in modo rapido.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicaz ione centrale all'inter no di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettaglia te sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitorag gio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitorano le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazioni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verificano eventi significativi. Il monitoraggio permette al carico di lavoro di riconoscere quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-6	Come si monitoran o le risorse del carico di lavoro? I log e le metriche sono strumenti molto efficaci per ottenere informazi oni sullo stato del carico di lavoro. Puoi configurare il carico di lavoro in modo da monitorare i log e le metriche e inviare notifiche quando vengono superate le soglie o si verifican o eventi significa tivi. Il monitoraggio permette al carico di lavoro di riconosce re quando vengono superate le soglie di prestazioni basse o si verificano errori, in modo che possa essere ripristinato automaticamente di rimando.	wafv2-logging-enab led	Per facilitare la registrazione e il monitoraggio all'inter no del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispon dente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-7	Come si progetta il carico di lavoro per adattarsi ai cambiamenti della domanda? Un carico di lavoro scalabile fornisce elasticità per aggiungere o rimuovere risorse automaticamente, in modo che vi sia una stretta corrispondenza con la domanda attuale in un dato momento.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-7	Come si progetta il carico di lavoro per adattarsi ai cambiamenti della domanda? Un carico di lavoro scalabile fornisce elasticità per aggiungere o rimuovere risorse automaticamente, in modo che vi sia una stretta corrispondenza con la domanda attuale in un dato momento.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-7	Come si progetta il carico di lavoro per adattarsi ai cambiamenti della domanda? Un carico di lavoro scalabile fornisce elasticità per aggiungere o rimuovere risorse automaticamente, in modo che vi sia una stretta corrispondenza con la domanda attuale in un dato momento.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-8	In che modo implementare le modifiche? Per implementare nuove funzionalità e verificare che i carichi di lavoro e l'ambiente operativo eseguano software noti e che sia possibile applicare patch o sostituirli in modo prevedibile, sono necessarie modifiche controllate. Se invece non sono controllate, risulta difficile prevederne l'effetto o risolvere eventuali problemi che causano.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-8	In che modo implementare le modifiche? Per implementare nuove funzionalità e verificare che i carichi di lavoro e l'ambiente operativo eseguano software noti e che sia possibile applicare patch o sostituirli in modo prevedibile, sono necessarie modifiche controllate. Se invece non sono controllate, risulta difficile prevederne l'effetto o risolvere eventuali problemi che causano.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-8	In che modo implementare le modifiche? Per implementare nuove funzionalità e verificare che i carichi di lavoro e l'ambiente operativo eseguano software noti e che sia possibile applicare patch o sostituirli in modo prevedibile, sono necessarie modifiche controllate. Se invece non sono controllate, risulta difficile prevederne l'effetto o risolvere eventuali problemi che causano.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-8	In che modo implementare le modifiche? Per implementare nuove funzionalità e verificare che i carichi di lavoro e l'ambiente operativo eseguano software noti e che sia possibile applicare patch o sostituirli in modo prevedibile, sono necessarie modifiche controllate. Se invece non sono controllate, risulta difficile prevederne l'effetto o risolvere eventuali problemi che causano.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazi oni e della configura zione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	backup-recovery-po int-minimum-retent ion-check	Per facilitare i processi di backup dei dati, assicurat i che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionD ays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazi oni e della configura zione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazi oni e della configura zione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazi oni e della configura zione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazi oni e della configura zione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazi oni e della configura zione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazi oni e della configura zione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazi oni e della configura zione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	rds-snapshot-encry pted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazi oni e della configura zione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazi oni e della configura zione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-9	In che modo eseguire il backup dei dati? Esegui il backup dei dati, delle applicazioni e della configurazione per soddisfare i requisiti relativi agli obiettivi del tempo di ripristino (RTO) e agli obiettivi del punto di ripristino (RPO).	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-10	Come si utilizza l'isolamento dei guasti per proteggere il carico di lavoro? Le barriere per l'isolamento dei guasti limitano l'effetto di un errore all'interno di un carico di lavoro a un numero limitato di componenti. I componenti al di fuori della barriera non subiscono gli effetti del guasto. Utilizzando più barriere per l'isolamento dei guasti, puoi limitare l'impatto sul carico di lavoro.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-10	Come si utilizza l'isolamento dei guasti per proteggere il carico di lavoro? Le barriere per l'isolamento dei guasti limitano l'effetto di un errore all'interno di un carico di lavoro a un numero limitato di componenti. I componenti al di fuori della barriera non subiscono gli effetti del guasto. Utilizzando più barriere per l'isolamento dei guasti, puoi limitare l'impatto sul carico di lavoro.	clb-multiple-az	Elastic Load Balancing (ELB) distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurati che ELB abbia registrato istanze da più zone di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-10	Come si utilizza l'isolamento dei guasti per proteggere il carico di lavoro? Le barriere per l'isolamento dei guasti limitano l'effetto di un errore all'interno di un carico di lavoro a un numero limitato di componenti. I componenti al di fuori della barriera non subiscono gli effetti del guasto. Utilizzando più barriere per l'isolamento dei guasti, puoi limitare l'impatto sul carico di lavoro.	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurati che ELB abbia registrato istanze da più zone di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-10	Come si utilizza l'isolamento dei guasti per proteggere il carico di lavoro? Le barriere per l'isolamento dei guasti limitano l'effetto di un errore all'interno di un carico di lavoro a un numero limitato di componenti. I componenti al di fuori della barriera non subiscono gli effetti del guasto. Utilizzando più barriere per l'isolamento dei guasti, puoi limitare l'impatto sul carico di lavoro.	lambda-vpc-multi-az-check	Se la tua funzione AWS Lambda è configurata per la connessione a un cloud privato virtuale (VPC) nel tuo account, implementa la funzione AWS Lambda in almeno due zone di disponibilità diverse per assicurarti che sia disponibile per elaborare gli eventi in caso di interruzione del servizio in una singola zona.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-10	Come si utilizza l'isolamento dei guasti per proteggere il carico di lavoro? Le barriere per l'isolamento dei guasti limitano l'effetto di un errore all'interno di un carico di lavoro a un numero limitato di componenti. I componenti al di fuori della barriera non subiscono gli effetti del guasto. Utilizzando più barriere per l'isolamento dei guasti, puoi limitare l'impatto sul carico di lavoro.	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) richiede almeno tre nodi di dati per un'elevata disponibilità e tolleranza ai guasti. L'implementazione di un dominio OpenSearch di servizio con almeno tre nodi di dati garantisce le operazioni del cluster in caso di guasto di un nodo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
REL-10	Come si utilizza l'isolamento dei guasti per proteggere il carico di lavoro? Le barriere per l'isolamento dei guasti limitano l'effetto di un errore all'interno di un carico di lavoro a un numero limitato di componenti. I componenti al di fuori della barriera non subiscono gli effetti del guasto. Utilizzando più barriere per l'isolamento dei guasti, puoi limitare l'impatto sul carico di lavoro.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
REL-10	Come si utilizza l'isolamento dei guasti per proteggere il carico di lavoro? Le barriere per l'isolamento dei guasti limitano l'effetto di un errore all'interno di un carico di lavoro a un numero limitato di componenti. I componenti al di fuori della barriera non subiscono gli effetti del guasto. Utilizzando più barriere per l'isolamento dei guasti, puoi limitare l'impatto sul carico di lavoro.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for AWS Well-Architected Reliability Pillar.

Best practice operative per AWS Well-Architected Framework Security Pillar

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra Well-Architected Framework Security Pillar di Amazon Web Services e le regole di Config gestite. AWS Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più principi di progettazione del pilastro. Una categoria del framework Well-Architected può essere correlata a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-1	Come gestire un carico di lavoro in sicurezza? Per gestire il carico di lavoro in modo sicuro, è necessario applicare le best practice globali a ogni area di sicurezza. Segui i requisiti e i processi definiti in termini di eccellenza operativa a livello organizzativo e di carico di lavoro e applicali a tutte	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	le aree. Rimanere aggiornati sulle raccomandazioni del settore AWS e sull'intelligence sulle minacce ti aiuta a far evolvere il tuo modello di minaccia e gli obiettivi di controllo. L'automazione dei processi di sicurezza, i test e la convalida permettono di dimensionare le operazioni di sicurezza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-1	Come gestire un carico di lavoro in sicurezza? Per gestire il carico di lavoro in modo sicuro, è necessario applicare le best practice globali a ogni area di sicurezza. Segui i requisiti e i processi definiti in termini di eccellenza operativa a livello organizzativo e di carico di lavoro e applicali a tutte le aree. Rimanere aggiornati sulle raccomandazioni del settore AWS e sull'intelligence sulle minacce aiuta a far evolvere il modello di minaccia e gli obiettivi di controllo. L'automazione dei processi di sicurezza, i test e la convalida permettono di dimensionare le operazioni di sicurezza.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-1	Come gestire un carico di lavoro in sicurezza? Per gestire il carico di lavoro in modo sicuro, è necessario applicare le best practice globali a ogni area di sicurezza. Segui i requisiti e i processi definiti in termini di eccellenza operativa a livello organizzativo e di carico di lavoro e applicali a tutte le aree. Rimanere aggiornati sulle raccomandazioni del settore AWS e sull'intelligence sulle minacce ti aiuta a far evolvere il tuo modello di minaccia e gli obiettivi di controllo. L'automazione dei processi di sicurezza, i test e la convalida permettono di dimensionare le operazioni di sicurezza.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-1	Come gestire un carico di lavoro in sicurezza? Per gestire il carico di lavoro in modo sicuro, è necessario applicare le best practice globali a ogni area di sicurezza. Segui i requisiti e i processi definiti in termini di eccellenza operativa a livello organizzativo e di carico di lavoro e applicali a tutte le aree. Rimanere aggiornati sulle raccomandazioni del settore AWS e sull'intelligence sulle minacce ti aiuta a far evolvere il tuo modello di minaccia e gli obiettivi di controllo. L'automazione dei processi di sicurezza, i test e la convalida permettono di dimensionare le operazioni di sicurezza.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-1	Come gestire un carico di lavoro in sicurezza? Per gestire il carico di lavoro in modo sicuro, è necessario applicare le best practice globali a ogni area di sicurezza. Segui i requisiti e i processi definiti in termini di eccellenza operativa a livello organizzativo e di carico di lavoro e applicali a tutte le aree. Rimanere aggiornati sulle raccomandazioni del settore AWS e sull'intelligence sulle minacce vi aiuta a far evolvere il vostro modello di minaccia e gli obiettivi di controllo. L'automazione dei processi di sicurezza, i test e la convalida permettono di dimensionare le operazioni di sicurezza.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-1	Come gestire un carico di lavoro in sicurezza? Per gestire il carico di lavoro in modo sicuro, è necessario applicare le best practice globali a ogni area di sicurezza. Segui i requisiti e i processi definiti in termini di eccellenza operativa a livello organizzativo e di carico di lavoro e applicali a tutte le aree. Rimanere aggiornati sulle raccomandazioni del settore AWS e sull'intelligence sulle minacce vi aiuta a far evolvere il vostro modello di minaccia e gli obiettivi di controllo. L'automazione dei processi di sicurezza, i test e la convalida permettono di dimensionare le operazioni di sicurezza.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-1	Come gestire un carico di lavoro in sicurezza? Per gestire il carico di lavoro in modo sicuro, è necessario applicare le best practice globali a ogni area di sicurezza. Segui i requisiti e i processi definiti in termini di eccellenza operativa a livello organizzativo e di carico di lavoro e applicali a tutte le aree. Rimanere aggiornati sulle raccomandazioni del settore AWS e sull'intelligence sulle minacce vi aiuta a far evolvere il vostro modello di minaccia e gli obiettivi di controllo. L'automazione dei processi di sicurezza, i test e la convalida permettono di dimensionare le operazioni di sicurezza.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-1	Come gestire un carico di lavoro in sicurezza? Per gestire il carico di lavoro in modo sicuro, è necessario applicare le best practice globali a ogni area di sicurezza. Segui i requisiti e i processi definiti in termini di eccellenza operativa a livello organizzativo e di carico di lavoro e applicali a tutte le aree. Rimanere aggiornati sulle raccomandazioni del settore AWS e sull'intelligence sulle minacce aiuta a far evolvere il modello di minaccia e gli obiettivi di controllo. L'automazione dei processi di sicurezza, i test e la convalida permettono di dimensionare le operazioni di sicurezza.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-1	Come gestire un carico di lavoro in sicurezza? Per gestire il carico di lavoro in modo sicuro, è necessario applicare le best practice globali a ogni area di sicurezza. Segui i requisiti e i processi definiti in termini di eccellenza operativa a livello organizzativo e di carico di lavoro e applicali a tutte le aree. Rimanere aggiornati sulle raccomandazioni del settore AWS e sull'intelligence sulle minacce aiuta a far evolvere il modello di minaccia e gli obiettivi di controllo. L'automazione dei processi di sicurezza, i test e la convalida permettono di dimensionare le operazioni di sicurezza.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-1	Come gestire un carico di lavoro in sicurezza? Per gestire il carico di lavoro in modo sicuro, è necessario applicare le best practice globali a ogni area di sicurezza. Segui i requisiti e i processi definiti in termini di eccellenza operativa a livello organizzativo e di carico di lavoro e applicali a tutte le aree. Rimanere aggiornati sulle raccomandazioni del settore AWS e sull'intelligence sulle minacce ti aiuta a far evolvere il tuo modello di minaccia e gli obiettivi di controllo. L'automazione dei processi di sicurezza, i test e la convalida permettono di dimensionare le operazioni di sicurezza.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità che devi gestire quando ti avvicini a carichi di lavoro operativi sicuri. AWS Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedono un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessitano dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri AWS . Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri. AWS Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri. AWS Comprende re il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificar e che le identità corrette abbiano accesso alle risorse giuste nelle condizion i adeguate. Identità umane: gli amministr atori, gli sviluppat ori, gli operatori e gli utenti finali richiedono un'identi tà per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazion e o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri AWS . Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri. AWS Comprende re il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificar e che le identità corrette abbiano accesso alle risorse giuste nelle condizion i adeguate. Identità umane: gli amministr atori, gli sviluppat ori, gli operatori e gli utenti finali richiedono un'identi tà per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazion e o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri AWS . Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri. AWS Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri. AWS Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri. AWS Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri AWS . Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri. AWS Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri. AWS Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri AWS . Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri. AWS Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	secretsmanager-secret-periodic-rotation	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione periodica abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto. Il valore predefinito è 90 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri. AWS Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	secretsmanager-secret-unused	Se in AWS Secrets Manager sono presenti credenziali inutilizzate, è necessario disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola consente di impostare un valore su unusedForDays (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri. AWS Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-2	Come si gestiscono le identità per persone e macchine? Esistono due tipi di identità da gestire quando si tratta di gestire carichi di lavoro sicuri. AWS Comprendere il tipo di identità necessaria per gestire e concedere l'accesso ti aiuta a verificare che le identità corrette abbiano accesso alle risorse giuste nelle condizioni adeguate. Identità umane: gli amministratori, gli sviluppatori, gli operatori e gli utenti finali richiedono un'identità per accedere agli ambienti e alle applicazioni. AWS Si tratta di membri dell'organizzazione o utenti esterni con cui collabora e che interagiscono con AWS le risorse dell'utente tramite un browser Web,	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	un'applicazione client o strumenti interattivi da riga di comando. Identità delle macchine: le applicazioni di servizio, gli strumenti operativi e i carichi di lavoro richiedon o un'identità per effettuare richieste ai AWS servizi, ad esempio per leggere i dati. Queste identità includono macchine in esecuzione nel tuo AWS ambiente, come istanze Amazon EC2 AWS o funzioni Lambda. Puoi gestire le identità di macchine anche per soggetti esterni che necessita no dell'accesso. Inoltre, potresti avere anche macchine esterne AWS che richiedono l'accesso al tuo ambiente. AWS		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegi o minimo, assicurat i che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	ecs-containers-non privileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizio ni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	ecs-containers-rea donly-access	L'abilitazione dell'acce sso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettar e il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificat o a meno che non disponga di autorizza zioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	efs-access-point-e nforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'uten te sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazion i sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti » con «Azione»: «*» rispetto a «Resource »: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti » con «Azione»: «*» rispetto a «Resource »: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	iam-user-group-membership-check	AWS Identity and Access Managemen t (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicuran do che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Ogni componente o risorsa del carico di lavoro deve essere accessibile da amministratori, utenti finali o altri componenti. Definisci chiaramente chi o cosa deve avere accesso a ciascun componente e scegli il tipo di identità e il metodo di autentica zione e autorizzazione appropriati.	iam-user-unused-cr edentials-check	AWS Identity and Access Managemen t (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controlla ndo le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizz ate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegi o minimo. Questa regola richiede di impostare un valore su maxCreden tialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Stabilisci controlli comuni che limitino l'accesso a tutte le identità della tua organizzazione. Ad esempio, puoi limitare l'accesso a AWS regioni specifiche o impedire agli operatori di eliminare risorse comuni, come un ruolo IAM utilizzat o per il tuo team di sicurezza centrale	account-part-of-or ganizations	La gestione centraliz zata Account AWS all'interno di AWS Organizations aiuta a garantire la conformit à degli account. L'assenza di una governance centraliz zata degli account può comportar e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuam ente i risultati che evidenziano l'accesso pubblico e multi-acc ount. Limita l'accesso pubblico e multi-acc ount alle risorse che lo richiedono.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuam ente i risultati che evidenziano l'accesso pubblico e multi-acc ount. Limita l'accesso pubblico e multi-acc ount alle risorse che lo richiedono.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuam ente i risultati che evidenziano l'accesso pubblico e multi-acc ount. Limita l'accesso pubblico e multi-acc ount alle risorse che lo richiedono.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicuran do che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuam ente i risultati che evidenziano l'accesso pubblico e multi-acc ount. Limita l'accesso pubblico e multi-acc ount alle risorse che lo richiedono.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuamente i risultati che evidenziano l'accesso pubblico e multi-account. Limita l'accesso pubblico e multi-account alle risorse che lo richiedono.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuamente i risultati che evidenziano l'accesso pubblico e multi-account. Limita l'accesso pubblico e multi-account alle risorse che lo richiedono.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuam ente i risultati che evidenziano l'accesso pubblico e multi-acc ount. Limita l'accesso pubblico e multi-acc ount alle risorse che lo richiedono.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuamente i risultati che evidenziano l'accesso pubblico e multi-account. Limita l'accesso pubblico e multi-account alle risorse che lo richiedono.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuam ente i risultati che evidenziano l'accesso pubblico e multi-acc ount. Limita l'accesso pubblico e multi-acc ount alle risorse che lo richiedono.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuam ente i risultati che evidenziano l'accesso pubblico e multi-acc ount. Limita l'accesso pubblico e multi-acc ount alle risorse che lo richiedono.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuam ente i risultati che evidenziano l'accesso pubblico e multi-acc ount. Limita l'accesso pubblico e multi-acc ount alle risorse che lo richiedono.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuam ente i risultati che evidenziano l'accesso pubblico e multi-acc ount. Limita l'accesso pubblico e multi-acc ount alle risorse che lo richiedono.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuamente i risultati che evidenziano l'accesso pubblico e multi-account. Limita l'accesso pubblico e multi-account alle risorse che lo richiedono.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuamente i risultati che evidenziano l'accesso pubblico e multi-account. Limita l'accesso pubblico e multi-account alle risorse che lo richiedono.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuamente i risultati che evidenziano l'accesso pubblico e multi-account. Limita l'accesso pubblico e multi-account alle risorse che lo richiedono.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuamente i risultati che evidenziano l'accesso pubblico e multi-account. Limita l'accesso pubblico e multi-account alle risorse che lo richiedono.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuamente i risultati che evidenziano l'accesso pubblico e multi-account. Limita l'accesso pubblico e multi-account alle risorse che lo richiedono.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuamente i risultati che evidenziano l'accesso pubblico e multi-account. Limita l'accesso pubblico e multi-account alle risorse che lo richiedono.	secretsmanager-secret-unused	Se in AWS Secrets Manager sono presenti credenziali inutilizzate, è necessario disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola consente di impostare un valore su unusedForDays (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuamente i risultati che evidenziano l'accesso pubblico e multi-account. Limita l'accesso pubblico e multi-account alle risorse che lo richiedono.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuam ente i risultati che evidenziano l'accesso pubblico e multi-acc ount. Limita l'accesso pubblico e multi-acc ount alle risorse che lo richiedono.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-3	Come si gestiscono le autorizzazioni per persone e macchine? Monitora continuam ente i risultati che evidenziano l'accesso pubblico e multi-acc ount. Limita l'accesso pubblico e multi-acc ount alle risorse che lo richiedono.	autoscaling-launch -config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribui re a rendere sicuro il carico di lavoro.	api-gw-execution-l ogging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-4	In che modo individui ed esamini gli eventi di sicurezza? Acquisisci e analizza gli eventi a partire da log e metriche per acquistare visibilità. Agisci su eventi di sicurezza e potenziali minacce per contribuire a rendere sicuro il carico di lavoro.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	ec2-instance-multiple-eni-check	Questa regola verifica se le istanze Amazon Elastic Compute Cloud (Amazon EC2) hanno più ENI. La presenza di più ENI può causare istanze dual-homed, ovvero istanze con più sottoreti. Ciò può aumentare la complessità della sicurezza della rete e introdurre percorsi e accessi di rete indesiderati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	waf-regional-rule-not-empty	Assicurati che il tuo AWS WAF abbia una regola che non sia vuota. Una regola senza condizioni può comportare un comportamento non intenzionale.
SEC-5	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	waf-regional-rulegroup-not-empty	Assicurati che il tuo AWS WAF abbia un gruppo di regole che non sia vuoto. Un gruppo di regole vuoto potrebbe causare un comportamento indesiderato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	waf-regional-webacl-not-empty	Un ACL Web collegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.
SEC-5	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventari o e una gestione accurati del proprio ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per proteggere da minacce esterne e interne basate sulla rete.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-5	In che modo proteggi le risorse di rete? Qualsiasi carico di lavoro che abbia una qualche forma di connettività di rete, che si tratti di Internet o di una rete privata, richiede più livelli di difesa per protegger e da minacce esterne e interne basate sulla rete.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	rds-automatic-mino r-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'install azione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relaziona le (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integri tà dei log. CloudTrai l La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificar e, eliminare o falsifica re i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribuire alla protezione e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenitori, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilita zione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribuire alla protezione e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenitori, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ecs-container-insights-enabled	Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon Elastic Container Service (ECS) e delle tue AWS soluzioni. Container Insights fornisce inoltre informazioni diagnostiche, ad esempio errori di riavvio del container, che consentono di isolare i problemi e risolverli in modo rapido.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribuiti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	redshift-cluster-m aintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizza zione. In particola re, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrad e Il valore predefini to è true. Inoltre, consente di impostare facoltativamente il preferredMaintenan ceWindow (l'impost azione predefinita è sab: 16:00 -sab: 16:30) e il automated SnapshotRetention periodo (l'impost azione predefinita è 1). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ec2-instance-multiple-eni-check	Questa regola verifica se le istanze Amazon Elastic Compute Cloud (Amazon EC2) hanno più ENI. La presenza di più ENI può causare istanze dual-home d, ovvero istanze con più sottoreti. Ciò può aumentare la complessità della sicurezza della rete e introdurre percorsi e accessi di rete indesiderati.
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicuran do che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribuire alla protezione e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenitori, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ec2-security-group -attached-to-eni-p eriodic	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambi ente.
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ec2-volume-inuse-c heck	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ec2-managedinstanc e-association-comp liance-status-check	Utilizza AWS Systems Manager Associati ons per semplific are l'inventario delle piattaforme e delle applicazioni software all'interno di un'organi zzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo , delle installaz ioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-6	In che modo proteggi le risorse di calcolo? Le risorse di calcolo nel carico di lavoro richiedono più livelli di difesa per contribui re alla protezion e da minacce esterne e interne. Le risorse di calcolo includono istanze EC2, contenito ri, funzioni AWS Lambda, servizi di database, dispositivi IoT e altro ancora.	ec2-managedinstanc e-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	codebuild-project-s3-logs-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per AWS CodeBuild i log archiviati in Amazon S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	kms-cmk-not-schedu led-for-deletion	Per proteggere i dati archiviati, assicurati che le chiavi master del cliente (CMK) necessarie non siano pianificate per l'eliminazione in AWS Key Managemen t Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificar e tutte le chiavi per le quali è pianifica ta l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzion ale.
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazi one predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	opensearch-encrypt ed-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	rds-snapshot-encry pted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	sagemaker-notebook -instance-kms-key- configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	secretsmanager-usi ng-cmk	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implementando più controlli per ridurre il rischio di accessi non autorizzati o altri comportamenti impropri.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	s3-account-level-p ublic-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltati vamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPubl icAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implementando più controlli per ridurre il rischio di accessi non autorizzati o altri comportamenti impropri.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implementando più controlli per ridurre il rischio di accessi non autorizzati o altri comportamenti impropri.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-8	Come proteggi i dati a riposo? Proteggi i dati a riposo implement ando più controlli per ridurre il rischio di accessi non autorizza ti o altri comportam enti impropri.	s3-bucket-public-w rite-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	acm-certificate-ex piration-check	Garantisci la protezion e dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExp iration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configura ti per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	s3-bucket-ssl-requ ests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizz o di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SEC-9	In che modo proteggi i dati in transito? Proteggi i dati in transito implement ando più controlli per ridurre il rischio di accessi non autorizza ti o perdita.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for AWS Well-Architected Security Pillar.

Best practice operative per BCP e DR

Questo pacchetto di conformità contiene AWS Config regole basate su BCP e DR all'interno. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle AWS Config regole gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for BCP and DR.

Best practice operative per BNM RMiT

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra le regole di Risk Management in Technology (RMiT) di Bank Negara Malaysia (BNM) e Config gestite. AWS Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli BNM RMit. Un controllo BNM RMiT può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazio ni di terzi, l'istituto finanziario valuta se tale affidamen to sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittogra fici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integri tà, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittogra fia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazio ni di terzi, l'istituto finanziario valuta se tale affidamen to sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittogra fici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integri tà, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittogra fia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazio ni di terzi, l'istituto finanziario valuta se tale affidamen to sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittogra fici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integri tà, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittogra fia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazio ni di terzi, l'istituto finanziario valuta se tale affidamen to sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittogra fici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integri tà, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittogra fia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazio ni di terzi, l'istituto finanziario valuta se tale affidamen to sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittogra fici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integri tà, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittogra fia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazio ni di terzi, l'istituto finanziario valuta se tale affidamen to sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittogra fici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integri tà, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittogra fia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazio ni di terzi, l'istituto finanziario valuta se tale affidamen to sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.18	Un istituto finanziario deve condurre la due diligence e valutare i controlli crittografici associati alla tecnologia utilizzata, al fine di proteggere la riservatezza, l'integrità, l'autenticazione, l'autorizzazione e garantire il non ripudio delle informazioni. Se un istituto finanziario non genera le proprie chiavi di crittografia, deve adottare le misure appropriate per garantire controlli e processi efficaci per la gestione delle chiavi di crittografia. Qualora ciò comporti il ricorso a valutazioni di terzi, l'istituto finanziario valuta se tale affidamento sia coerente con la propensione e la tolleranza al rischio dell'istituto finanziario. Un istituto finanziario deve inoltre prestare la dovuta attenzion	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e alle risorse di sistema necessari e per supportare i controlli crittografici e al rischio di una ridotta visibilità del traffico di rete dei dati non crittografati.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.20	Un istituto finanziario deve archiviare le chiavi di crittografia pubbliche in un certificato rilasciato da un'autorità di certificazione in base al livello di rischio. Tali certificati associati ai clienti devono essere rilasciati da autorità di certificazione riconosciute. L'istituto finanziario deve garantire che l'implementazione dei protocolli di autenticazione e firma che utilizzano tali certificati sia soggetta a un livello di protezione elevato per garantire che l'uso delle chiavi di crittografia private corrispondenti ai certificati dell'utente sia giuridicamente vincolante e irrefutabile. L'emissione iniziale e il successivo rinnovo di tali certificati devono essere coerenti con le best	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	practice del settore e le specifiche legali/normative applicabili.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.20	Un istituto finanziario deve archiviare le chiavi di crittografia pubbliche in un certificato rilasciato da un'autorità di certificazione in base al livello di rischio. Tali certificati associati ai clienti devono essere rilasciati da autorità di certificazione riconosciute. L'istituto finanziario deve garantire che l'implementazione dei protocolli di autenticazione e firma che utilizzano tali certificati sia soggetta a un livello di protezione elevato per garantire che l'uso delle chiavi di crittografia private corrispondenti ai certificati dell'utente sia giuridicamente vincolante e irrefutabile. L'emissione iniziale e il successivo rinnovo di tali certificati devono essere coerenti con le best	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	practice del settore e le specifiche legali/normative applicabili.		
10.27	Un istituto finanziario deve stabilire meccanismi di monitoraggio in tempo reale per tenere traccia dell'utilizzo della capacità e delle prestazioni dei processi e dei servizi principali. Questi meccanismi di monitoraggio devono essere progettati per fornire avvisi tempestivi e utilizzabili agli amministratori.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,27	Un istituto finanziario deve stabilire meccanismi di monitoraggio in tempo reale per tenere traccia dell'utilizzo della capacità e delle prestazioni dei processi e dei servizi principali. Questi meccanismi di monitoraggio devono essere progettati per fornire avvisi tempestivi e utilizzabili agli amministratori.	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.27	Un istituto finanziar io deve stabilire meccanismi di monitoraggio in tempo reale per tenere traccia dell'util izzo della capacità e delle prestazioni dei processi e dei servizi principali. Questi meccanismi di monitoraggio devono essere progettat i per fornire avvisi tempestivi e utilizzabili agli amministratori.	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.27	Un istituto finanziar io deve stabilire meccanismi di monitoraggio in tempo reale per tenere traccia dell'util izzo della capacità e delle prestazioni dei processi e dei servizi principali. Questi meccanismi di monitoraggio devono essere progettat i per fornire avvisi tempestivi e utilizzabili agli amministratori.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.27	Un istituto finanziario deve stabilire meccanismi di monitoraggio in tempo reale per tenere traccia dell'utilizzo della capacità e delle prestazioni dei processi e dei servizi principali. Questi meccanismi di monitoraggio devono essere progettati per fornire avvisi tempestivi e utilizzabili agli amministratori.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
10.27	Un istituto finanziario deve stabilire meccanismi di monitoraggio in tempo reale per tenere traccia dell'utilizzo della capacità e delle prestazioni dei processi e dei servizi principali. Questi meccanismi di monitoraggio devono essere progettati per fornire avvisi tempestivi e utilizzabili agli amministratori.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,27	Un istituto finanziario deve stabilire meccanismi di monitoraggio in tempo reale per tenere traccia dell'utilizzo della capacità e delle prestazioni dei processi e dei servizi principali. Questi meccanismi di monitoraggio devono essere progettati per fornire avvisi tempestivi e utilizzabili agli amministratori.	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,27	Un istituto finanziario deve stabilire meccanismi di monitoraggio in tempo reale per tenere traccia dell'utilizzo della capacità e delle prestazioni dei processi e dei servizi principali. Questi meccanismi di monitoraggio devono essere progettati per fornire avvisi tempestivi e utilizzabili agli amministratori.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.27	Un istituto finanziario deve stabilire meccanismi di monitoraggio in tempo reale per tenere traccia dell'utilizzo della capacità e delle prestazioni dei processi e dei servizi principali. Questi meccanismi di monitoraggio devono essere progettati per fornire avvisi tempestivi e utilizzabili agli amministratori.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,34	Un istituto finanziario deve garantire che i servizi di rete per i suoi sistemi critici siano affidabili e privi di singoli punti di errore (SPOF) per proteggere i sistemi critici da potenziali guasti di rete e minacce informatiche.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,34	Un istituto finanziario deve garantire che i servizi di rete per i suoi sistemi critici siano affidabili e privi di singoli punti di errore (SPOF) per proteggere i sistemi critici da potenziali guasti di rete e minacce informatiche.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,35	Un istituto finanziario deve stabilire processi di monitoraggio della larghezza di banda della rete in tempo reale e i corrispondenti parametri di resilienza dei servizi di rete per segnalare eventuali utilizzi eccessivi della larghezza di banda e interruzioni del sistema dovute a congestione della larghezza di banda e guasti di rete. Uno di questi processi è l'analisi del traffico per rilevare tendenze e anomalie.	api-gw-xray-enabled	AWS X-Ray raccoglie dati sulle richieste servite dall'applicazione e fornisce strumenti che è possibile utilizzare per visualizzare, filtrare e acquisire informazioni su tali dati per identificare problemi e opportunità di ottimizzazione. Assicurati che X-Ray sia abilitato in modo da poter visualizzare informazioni dettagliate non solo sulla richiesta e sulla risposta, ma anche sulle chiamate effettuate dall'applicazione a AWS risorse downstream, microservizi, database e API Web HTTP.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.35	Un istituto finanziario deve stabilire processi di monitoraggio della larghezza di banda della rete in tempo reale e i corrispondenti parametri di resilienza dei servizi di rete per segnalare eventuali utilizzi eccessivi della larghezza di banda e interruzioni del sistema dovute a congestione della larghezza di banda e guasti di rete. Uno di questi processi è l'analisi del traffico per rilevare tendenze e anomalie.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.35	Un istituto finanziario deve stabilire processi di monitoraggio della larghezza di banda della rete in tempo reale e i corrispondenti parametri di resilienza dei servizi di rete per segnalare eventuali utilizzi eccessivi della larghezza di banda e interruzioni del sistema dovute a congestione della larghezza di banda e guasti di rete. Uno di questi processi è l'analisi del traffico per rilevare tendenze e anomalie.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,35	Un istituto finanziario deve stabilire processi di monitoraggio della larghezza di banda della rete in tempo reale e i corrispondenti parametri di resilienza dei servizi di rete per segnalare eventuali utilizzi eccessivi della larghezza di banda e interruzioni del sistema dovute a congestione della larghezza di banda e guasti di rete. Uno di questi processi è l'analisi del traffico per rilevare tendenze e anomalie.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,36	Un istituto finanziario deve garantire che i servizi di rete che supportano i sistemi critici siano progettati e implementati per garantire la riservatezza, l'integrità e la disponibilità dei dati.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
10,36	Un istituto finanziario deve garantire che i servizi di rete che supportano i sistemi critici siano progettati e implementati per garantire la riservatezza, l'integrità e la disponibilità dei dati.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,36	Un istituto finanziario deve garantire che i servizi di rete che supportano i sistemi critici siano progettati e implementati per garantire la riservatezza, l'integrità e la disponibilità dei dati.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
10.36	Un istituto finanziario deve garantire che i servizi di rete che supportano i sistemi critici siano progettati e implementati per garantire la riservatezza, l'integrità e la disponibilità dei dati.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,36	Un istituto finanziario deve garantire che i servizi di rete che supportano i sistemi critici siano progettati e implementati per garantire la riservatezza, l'integrità e la disponibilità dei dati.	nlb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per i tuoi Network Load Balancer (NLB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,38	Un istituto finanziario deve garantire che venga mantenuto un numero sufficiente di log pertinenti ai dispositivi di rete per indagini e scopi forensi per almeno tre anni.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	autoscaling-launch -config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti IAM siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti IAM. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti di account compromes si richiedendo l'autenti cazione a più fattori per gli utenti IAM.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	opensearch-https-r equired	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearc h Service all'inter no di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	root-account-hardw are-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	root-account-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	sagemaker-endpoint -configuration-kms- key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezion e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardan ti clienti e contropar ti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinent i.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.51	Quando utilizza servizi cloud, un istituto finanziario deve implementare misure di protezione e adeguate per le informazioni di clienti e controparti e per i dati proprietari al fine di impedirne la divulgazione e gli accessi non autorizzati. Queste misure includono il mantenimento della proprietà, del controllo e della gestione di tutti i dati relativi alle informazioni riguardanti clienti e controparti, dei dati e servizi proprietari ospitati sul cloud, inclusa la gestione delle chiavi di crittografia pertinenti.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziario deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprendere i controlli degli accessi alla tecnologia sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziario deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprendere i controlli degli accessi alla tecnologia sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziar io deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprende re i controlli degli accessi alla tecnologi a sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,52	Un istituto finanziar io deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprende re i controlli degli accessi alla tecnologi a sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,52	Un istituto finanziar io deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprende re i controlli degli accessi alla tecnologi a sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziario deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprendere i controlli degli accessi alla tecnologia sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziario deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprendere i controlli degli accessi alla tecnologia sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziario deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprendere i controlli degli accessi alla tecnologia sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziar io deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprende re i controlli degli accessi alla tecnologi a sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziario deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprendere i controlli degli accessi alla tecnologia sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti IAM siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziario deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprendere i controlli degli accessi alla tecnologia sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti IAM. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti di account compromessi richiedendo l'autenticazione a più fattori per gli utenti IAM.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziario deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprendere i controlli degli accessi alla tecnologia sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziario deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprendere i controlli degli accessi alla tecnologia sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziario deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprendere i controlli degli accessi alla tecnologia sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.52	Un istituto finanziario deve attuare un'adeguata policy di controllo degli accessi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (utenti interni ed esterni, come ad esempio fornitori di servizi terzi). La policy deve comprendere i controlli degli accessi alla tecnologia sia logici sia fisici, commisurati al livello di rischio di accessi non autorizzati a tali sistemi tecnologici.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.53(b)(h)(i)	Nel rispettare il paragrafo 10.52, un istituto finanziar io deve prendere in considerazione i seguenti principi nella sua policy di controllo degli accessi: (b) utilizzare i diritti di accesso con "privilegio minimo" o "necessario", laddove agli utenti legittimi siano concesse solo le autorizzazioni minime sufficienti per svolgere i loro ruoli; (h) limitare e controlla re la condivisione di ID utente e password tra più utenti; e (i) controllare l'uso di convenzioni generiche di denominazione degli ID utente a favore di ID che consentano un'identi ficazione personale maggiore.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.53(b)	Nell'osservare il paragrafo 10.52, un istituto finanziar io deve prendere in considerazione i seguenti principi nella sua policy di controllo degli accessi: (b) utilizzare i diritti di accesso con "privilegio minimo" o "necessari", laddove agli utenti legittimi siano concesse solo le autorizzazioni minime sufficienti per svolgere i loro ruoli;	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.53(b)	Nell'osservare il paragrafo 10.52, un istituto finanziar io deve prendere in considerazione i seguenti principi nella sua policy di controllo degli accessi: (b) utilizzare i diritti di accesso con "privilegio minimo" o "necessari", laddove agli utenti legittimi siano concesse solo le autorizzazioni minime sufficienti per svolgere i loro ruoli;	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.53(b)	Nell'osservare il paragrafo 10.52, un istituto finanziar io deve prendere in considerazione i seguenti principi nella sua policy di controllo degli accessi: (b) utilizzare i diritti di accesso con "privilegio minimo" o "necessari", laddove agli utenti legittimi siano concesse solo le autorizzazioni minime sufficienti per svolgere i loro ruoli;	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.53(b)	Nell'osservare il paragrafo 10.52, un istituto finanziar io deve prendere in considerazione i seguenti principi nella sua policy di controllo degli accessi: (b) utilizzare i diritti di accesso con "privilegio minimo" o "necessari", laddove agli utenti legittimi siano concesse solo le autorizzazioni minime sufficienti per svolgere i loro ruoli;	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.53(b)	Nell'osservare il paragrafo 10.52, un istituto finanziario deve prendere in considerazione i seguenti principi nella sua policy di controllo degli accessi: (b) utilizzare i diritti di accesso con "privilegio minimo" o "necessari", laddove agli utenti legittimi siano concesse solo le autorizzazioni minime sufficienti per svolgere i loro ruoli;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.53(b)	Nell'osservare il paragrafo 10.52, un istituto finanziario deve prendere in considerazione i seguenti principi nella sua policy di controllo degli accessi: (b) utilizzare i diritti di accesso con "privilegio minimo" o "necessari", laddove agli utenti legittimi siano concesse solo le autorizzazioni minime sufficienti per svolgere i loro ruoli;	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti IAM siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.53(b)	Nell'osservare il paragrafo 10.52, un istituto finanziar io deve prendere in considerazione i seguenti principi nella sua policy di controllo degli accessi: (b) utilizzare i diritti di accesso con "privilegio minimo" o "necessari", laddove agli utenti legittimi siano concesse solo le autorizzazioni minime sufficienti per svolgere i loro ruoli;	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.53(c)(f)	Nell'osservare il paragrafo 10.52, un istituto finanziario deve prendere in considerare i seguenti principi nella sua policy di controllo degli accessi: (c) utilizzare diritti di accesso limitati nel tempo che restringa no l'accesso a un periodo specifico, compresi i diritti di accesso concessi ai fornitori di servizi; (f) adottare una modalità di autenticazione più rigorosa per le attività critiche, incluso l'accesso remoto	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.53(f)(h)	Nell'osservare il paragrafo 10.52, un istituto finanziar io deve prendere in considerazione i seguenti principi nella sua policy di controllo degli accessi: (f) adottare un'autent icazione più rigorosa per le attività critiche, incluso l'accesso remoto; (h) limitare e controllare la condivisi one di ID utente e password tra più utenti	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti IAM. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti di account compromes si richiedendo l'autenti cazione a più fattori per gli utenti IAM.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.53(f)(h)	Nell'osservare il paragrafo 10.54, un istituto finanziario deve prendere in considerazione i seguenti principi nella sua policy di controllo degli accessi: (f) adottare un'autenticazione più rigorosa per le attività critiche, incluso l'accesso remoto; (h) limitare e controllare la condivisione di ID utente e password tra più utenti	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.53(f)(h)	Nell'osservare il paragrafo 10.54, un istituto finanziar io deve prendere in considerazione i seguenti principi nella sua policy di controllo degli accessi: (f) adottare un'autent icazione più rigorosa per le attività critiche, incluso l'accesso remoto; (h) limitare e controllare la condivisi one di ID utente e password tra più utenti	root-account-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.54	Un istituto finanziario deve utilizzare processi di autenticazione efficaci per garantire l'autenticità delle identità in uso. I meccanismi di autenticazione devono essere commisurati alla criticità delle funzioni e adottare almeno uno o più di questi tre fattori di autenticazione di base, vale a dire qualcosa che l'utente conosce (ad esempio password, PIN), qualcosa che l'utente possiede (ad esempio smart card, dispositivo di sicurezza) e qualcosa che l'utente è (ad esempio caratteristiche biometriche, come un'impronta digitale o uno schema retinico).	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel Cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti IAM. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti di account compromessi richiedendo l'autenticazione a più fattori per gli utenti IAM.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.54	Un istituto finanziario deve utilizzare processi di autenticazione efficaci per garantire l'autenticità delle identità in uso. I meccanismi di autenticazione devono essere commisurati alla criticità delle funzioni e adottare almeno uno o più di questi tre fattori di autenticazione di base, vale a dire qualcosa che l'utente conosce (ad esempio password, PIN), qualcosa che l'utente possiede (ad esempio smart card, dispositivo di sicurezza) e qualcosa che l'utente è (ad esempio caratteristiche biometriche, come un'impronta digitale o uno schema retinico).	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.54	Un istituto finanziario deve utilizzare processi di autenticazione efficaci per garantire l'autenticità delle identità in uso. I meccanismi di autenticazione devono essere commisurati alla criticità delle funzioni e adottare almeno uno o più di questi tre fattori di autenticazione di base, vale a dire qualcosa che l'utente conosce (ad esempio password, PIN), qualcosa che l'utente possiede (ad esempio smart card, dispositivo di sicurezza) e qualcosa che l'utente è (ad esempio caratteristiche biometriche, come un'impronta digitale o uno schema retinico).	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.55	Un istituto finanziario deve rivedere e adattare periodicamente le proprie pratiche in materia di password per migliorare la resilienza contro gli attacchi in evoluzione. Ciò include la generazione efficace e sicura di password. Inoltre, l'istituto deve mettere in atto i controlli appropriati per verificare la sicurezza delle password create.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.56	Generalmente, i metodi di autentica zione basati su più di un fattore sono più difficili da compromettere rispetto a un sistema a fattore singolo. In considerazione di ciò, gli istituti finanziar i sono incoraggi ati a progettare e implementare correttamente (soprattutto nei sistemi ad alto rischio o ad autenticazione unica) l'autenticazione a più fattori (MFA), che garantisce maggiore affidabilità e fornisce deterrenti più efficaci contro le frodi	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti IAM. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti di account compromes si richiedendo l'autenti cazione a più fattori per gli utenti IAM.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.56	Generalmente, i metodi di autentica zione basati su più di un fattore sono più difficili da compromettere rispetto a un sistema a fattore singolo. In considerazione di ciò, gli istituti finanziar i sono incoraggi ati a progettare e implementare correttamente (soprattutto nei sistemi ad alto rischio o ad autenticazione unica) l'autenticazione a più fattori (MFA), che garantisce maggiore affidabilità e fornisce deterrenti più efficaci contro le frodi	root-account-hardw are-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.56	Generalmente, i metodi di autentica zione basati su più di un fattore sono più difficili da compromettere rispetto a un sistema a fattore singolo. In considerazione di ciò, gli istituti finanziar i sono incoraggi ati a progettare e implementare correttamente (soprattutto nei sistemi ad alto rischio o ad autenticazione unica) l'autenticazione a più fattori (MFA), che garantisce maggiore affidabilità e fornisce deterrenti più efficaci contro le frodi	root-account-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	cw-loggroup-retent ion-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzio ne dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruz ione e l'identificazione di eventi potenzial mente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti IAM siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,59	Un istituto finanziario deve garantire che (a) i controlli di accesso ai sistemi a livello aziendale siano gestiti e monitorati in modo efficace; e che (b) le attività degli utenti nei sistemi critici siano registrate per fini di audit e indagine. I log delle attività devono essere conservati per almeno tre anni e rivisti regolarmente in modo tempestivo.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.60	Nel soddisfare il requisito di cui al paragrafo 10.59, gli istituti finanziari di grandi dimension i sono tenuti a (a) implementare un sistema di gestione degli accessi alle identità per gestire e monitorare efficacem ente l'accesso degli utenti ai sistemi a livello aziendale; e (b) implementare strumenti di audit automatizzati per segnalare eventuali anomalie.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.60	Nel soddisfare il requisito di cui al paragrafo 10.61, gli istituti finanziari di grandi dimension i sono tenuti a (a) implementare un sistema di gestione degli accessi alle identità per gestire e monitorare efficacem ente l'accesso degli utenti ai sistemi a livello aziendale; e (b) implementare strumenti di audit automatizzati per segnalare eventuali anomalie.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.60	Nel soddisfare il requisito di cui al paragrafo 10.61, gli istituti finanziari di grandi dimension i sono tenuti a (a) implementare un sistema di gestione degli accessi alle identità per gestire e monitorare efficacem ente l'accesso degli utenti ai sistemi a livello aziendale; e (b) implementare strumenti di audit automatizzati per segnalare eventuali anomalie.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.61	Un istituto finanziario deve garantire che i sistemi critici non funzionino su sistemi obsoleti con vulnerabilità di sicurezza note o sistemi tecnologici end-of-life (EOL). A questo proposito, un istituto finanziario deve assegnare in modo chiaro le responsabilità alle funzioni identificate: (a) monitorare e continuamente e implementare in maniera tempestiva le ultime versioni delle patch; e (b) identificare i sistemi tecnologici critici che si avvicinano alla fine del ciclo di vita (EOL) per ulteriori azioni correttive.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.61	Un istituto finanziario deve garantire che i sistemi critici non funzionino su sistemi obsoleti con vulnerabilità di sicurezza note o sistemi tecnologici end-of-life (EOL). A questo proposito, un istituto finanziario deve assegnare in modo chiaro le responsabilità alle funzioni identificate: (a) monitorare e continuamente e implementare in maniera tempestiva le ultime versioni delle patch; e (b) identificare i sistemi tecnologici critici che si avvicinano alla fine del ciclo di vita (EOL) per ulteriori azioni correttive.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.61	Un istituto finanziario deve garantire che i sistemi critici non funzionino su sistemi obsoleti con vulnerabilità di sicurezza note o sistemi tecnologici end-of-life (EOL). A questo proposito, un istituto finanziario deve assegnare in modo chiaro le responsabilità alle funzioni identificate: (a) monitorare e continuamente e implementare in maniera tempestiva le ultime versioni delle patch; e (b) identificare i sistemi tecnologici critici che si avvicinano alla fine del ciclo di vita (EOL) per ulteriori azioni correttive.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.61	Un istituto finanziario deve garantire che i sistemi critici non funzionino su sistemi obsoleti con vulnerabilità di sicurezza note o sistemi tecnologici end-of-life (EOL). A questo proposito, un istituto finanziario deve assegnare in modo chiaro le responsabilità alle funzioni identificate: (a) monitorare e continuamente e implementare in maniera tempestiva le ultime versioni delle patch; e (b) identificare i sistemi tecnologici critici che si avvicinano alla fine del ciclo di vita (EOL) per ulteriori azioni correttive.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.61	Un istituto finanziario deve garantire che i sistemi critici non funzionino su sistemi obsoleti con vulnerabilità di sicurezza note o sistemi tecnologici end-of-life (EOL). A questo proposito, un istituto finanziario deve assegnare in modo chiaro le responsabilità alle funzioni identificate: (a) monitorare e continuamente e implementare in maniera tempestiva le ultime versioni delle patch; e (b) identificare i sistemi tecnologici critici che si avvicinano alla fine del ciclo di vita (EOL) per ulteriori azioni correttive.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	rds-snapshot-encry pted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizz o di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	sagemaker-endpoint -configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	sagemaker-notebook -instance-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	secretsmanager-usi ng-cmk	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(a)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (a) la riservate zza e l'integrità delle informazioni e delle transazioni dei clienti e delle controparti	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(b)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (b) affidabil ità dei servizi forniti tramite canali e dispositivi con interruzioni minime dei servizi	dynamodb-autoscali ng-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automatic amente ai modelli di traffico effettivi . In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvis i aumenti di traffico, senza alcuna limitazio ne (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(b)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (b) affidabil ità dei servizi forniti tramite canali e dispositivi con interruzioni minime dei servizi	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.
10.64(b)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (b) affidabil ità dei servizi forniti tramite canali e dispositivi con interruzioni minime dei servizi	elb-deletion-prote ction-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciam ento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(b)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (b) affidabil ità dei servizi forniti tramite canali e dispositivi con interruzioni minime dei servizi	nlb-cross-zone-load-balancing-enabled	Abilita il bilanciam ento del carico tra zone per i tuoi sistemi di bilanciam ento (NetworkLoad NLB) per mantenere capacità e disponibi lità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(b)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (b) affidabil ità dei servizi forniti tramite canali e dispositivi con interruzioni minime dei servizi	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(b)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (b) affidabil ità dei servizi forniti tramite canali e dispositivi con interruzioni minime dei servizi	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
10.64(b)	Nella fornitura di servizi digitali, un istituto finanziario deve implementare efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (b) affidabilità dei servizi forniti tramite canali e dispositivi con interruzioni minime dei servizi	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	api-gw-execution-l ogging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	dynamodb-throughpu t-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissi one assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportar e. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficien ti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissi one effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltati vamente i parametri AccountRCU ThresholdPercentag e (Config Default: 80) e AccountWCU ThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitorag gio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicaz ione centrale all'inter no di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettaglia te sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearc h di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearc h I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosti care problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	rds-enhanced-monit oring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorar e la disponibilità di Amazon RDS. Ciò fornisce una visibilit à dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archivi azione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositi vo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(d)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (d) sufficiente audit trail e monitorag gio delle transazioni anomale	wafv2-logging-enab led	Per facilitare la registrazione e il monitoraggio all'inter no del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispon dente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	dynamodb-pitr-enab led	Abilita questa regola per verificare che sia stato eseguito il backup delle informazi oni. Inoltre, mantiene i backup assicuran do che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristin o mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	ebs-optimized-inst ance	Un'istanza ottimizza ta in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/ O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	ebs-resources-prot ected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	efs-resources-prot ected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	rds-resources-prot ected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	redshift-backup-en abled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatiz zati. Quando gli snapshot automatic i sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazi one predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.64(e)	Nella fornitura di servizi digitali, un istituto finanziario deve implement are efficaci controlli di sicurezza della tecnologia che garantiscano quanto segue: (e) la capacità di identificare e ristabilire il punto di ripristino prima dell'incidente o dell'interruzione del servizio	s3-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i bucket Amazon Simple Storage Service (S3) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.7	Un istituto finanziario deve implementare strumenti efficaci per supportare il monitoraggio continuo e proattivo e il rilevamento tempestivo di attività anomale nella propria infrastruttura tecnologica. L'ambito del monitoraggio deve coprire tutti i sistemi critici, inclusa l'infrastruttura di supporto.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.7	Un istituto finanziar io deve implement are strumenti efficaci per supportare il monitoraggio continuo e proattivo e il rilevamento tempestivo di attività anomale nella propria infrastruttura tecnologi ca. L'ambito del monitoraggio deve coprire tutti i sistemi critici, inclusa l'infrast ruttura di supporto.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.8	Un istituto finanziario deve garantire che le proprie operazioni di sicurezza informatica prevengano e rilevino in maniera continua qualsiasi potenziale compromissione dei controlli di sicurezza o indebolimento del proprio livello di sicurezza. Per gli istituti finanziari di grandi dimensioni, ciò deve includere l'esecuzione di una valutazione trimestrale della vulnerabilità dei componenti di rete esterni e interni che supportano tutti i sistemi critici.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.8	Un istituto finanziario deve garantire che le proprie operazioni di sicurezza informatica prevengano e rilevino in maniera continua qualsiasi potenziale compromissione dei controlli di sicurezza o indebolimento del proprio livello di sicurezza. Per gli istituti finanziari di grandi dimensioni, ciò deve includere l'esecuzione di una valutazione trimestrale della vulnerabilità dei componenti di rete esterni e interni che supportano tutti i sistemi critici.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.18(c)(f)	Il centro per le operazioni di sicurezza (SOC) deve essere in grado di svolgere le seguenti funzioni: (c) gestione delle vulnerabilità; (f) fornitura di consapevolezza situazionale per rilevare avversari e minacce, comprese l'analisi e le operazioni di intelligence sulle minacce e il monitoraggio degli indicatori di compromissione (IOC). Ciò include un'analisi comportamentale avanzata per rilevare malware in assenza di firma e di file e per identificare anomalie che possono rappresentare minacce alla sicurezza, anche a livello di endpoint e di rete.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.18(c)(f)	Il centro per le operazioni di sicurezza (SOC) deve essere in grado di svolgere le seguenti funzioni: (c) gestione delle vulnerabilità; (f) fornitura di consapevolezza situazionale per rilevare avversari e minacce, comprese l'analisi e le operazioni di intelligence sulle minacce e il monitoraggio degli indicatori di compromissione (IOC). Ciò include un'analisi comportamentale avanzata per rilevare malware in assenza di firma e di file e per identificare anomalie che possono rappresentare minacce alla sicurezza, anche a livello di endpoint e di rete.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.18(c)(f)	Il centro per le operazioni di sicurezza (SOC) deve essere in grado di svolgere le seguenti funzioni: (c) gestione delle vulnerabilità; (f) fornitura di consapevolezza situazionale per rilevare avversari e minacce, comprese l'analisi e le operazioni di intelligence sulle minacce e il monitoraggio degli indicatori di compromissione (IOC). Ciò include un'analisi comportamentale avanzata per rilevare malware in assenza di firma e di file e per identificare anomalie che possono rappresentare minacce alla sicurezza, anche a livello di endpoint e di rete.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.1	Effettuare una revisione periodica della configurazione e delle impostazioni delle regole per tutti i dispositivi di sicurezza . Utilizzare strumenti automatizzati per rivedere e monitorar e le modifiche alla configurazione e alle impostazioni delle regole.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.1	Effettuare una revisione periodica della configurazione e delle impostazioni delle regole per tutti i dispositivi di sicurezza . Utilizzare strumenti automatizzati per rivedere e monitorar e le modifiche alla configurazione e alle impostazioni delle regole.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.5(b)	Garantisci che i controlli di sicurezza per le connessioni di rete server-to-server esterne includano quanto segue: (b) uso di tunnel sicuri come Transport Layer Security (TLS) e Virtual Private Network (VPN) IPSec	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
Appendice 5.5(b)	Garantire che i controlli di sicurezza per le connessioni di rete server-to-server esterne includano quanto segue: (b) uso di tunnel sicuri come Transport Layer Security (TLS) e Virtual Private Network (VPN) IPSec	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.5(b)	Garantire che i controlli di sicurezza per le connessioni di rete server-to-server esterne includano quanto segue: (b) uso di tunnel sicuri come Transport Layer Security (TLS) e Virtual Private Network (VPN) IPSec	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
Appendice 5.5(b)	Assicurati che i controlli di sicurezza per le connessioni di rete server-to-server esterne includano quanto segue: (b) utilizzo di tunnel sicuri come Transport Layer Security (TLS) e Virtual Private Network (VPN) IPSec	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.5(b)	Garantisci che i controlli di sicurezza per le connessioni di rete server-to-server esterne includano quanto segue: (b) uso di tunnel sicuri come Transport Layer Security (TLS) e Virtual Private Network (VPN) IPSec	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Appendice 5.5(b)	Garantire che i controlli di sicurezza per le connessioni di rete server-to-server esterne includano quanto segue: (b) uso di tunnel sicuri come Transport Layer Security (TLS) e Virtual Private Network (VPN) IPSec	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.5(c)	Assicuratevi che i controlli di sicurezza per le connessioni di rete server-to-server esterne includano quanto segue: (c) implementazione di server di staging con difese e protezioni perimetrali adeguate come firewall, IPS e antivirus.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.5(c)	Assicurati che i controlli di sicurezza per le connessioni di rete server-to-server esterne includano quanto segue: (c) implementazione di server di staging con difese e protezioni perimetrali adeguate come firewall, IPS e antivirus.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.5(c)	Assicuratevi che i controlli di sicurezza per le connessioni di rete server-to-server esterne includano quanto segue: (c) implementazione di server di staging con difese e protezioni perimetrali adeguate come firewall, IPS e antivirus.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.6	Garantire che i controlli di sicurezza per l'accesso remoto al server includano quanto segue: (a) limitazione dell'acce sso solo ai dispositi vi endpoint protetti e bloccati; (b) utilizzo di tunnel sicuri come TLS e VPN IPSec; (c) implementazione di un server "gateway" con difese e protezion i perimetrali adeguate come firewall, IPS e antivirus; e (d) chiusura delle porte interessate immediata mente dopo la scadenza dell'acce sso remoto.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.6	Garantire che i controlli di sicurezza per l'accesso remoto al server includano quanto segue: (a) limitazione dell'accesso solo ai dispositivi endpoint protetti e bloccati; (b) utilizzo di tunnel sicuri come TLS e VPN IPSec; (c) implementazione di un server "gateway" con difese e protezioni perimetrali adeguate come firewall, IPS e antivirus; e (d) chiusura delle porte interessate immediatamente dopo la scadenza dell'accesso remoto.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.6	Garantire che i controlli di sicurezza per l'accesso remoto al server includano quanto segue: (a) limitazione dell'accesso solo ai dispositivi endpoint protetti e bloccati; (b) utilizzo di tunnel sicuri come TLS e VPN IPSec; (c) implementazione di un server "gateway" con difese e protezioni perimetrali adeguate come firewall, IPS e antivirus; e (d) chiusura delle porte interessate immediatamente dopo la scadenza dell'accesso remoto.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.6	Garantire che i controlli di sicurezza per l'accesso remoto al server includano quanto segue: (a) limitazione dell'accesso solo ai dispositivi endpoint protetti e bloccati; (b) utilizzo di tunnel sicuri come TLS e VPN IPSec; (c) implementazione di un server "gateway" con difese e protezioni perimetrali adeguate come firewall, IPS e antivirus; e (d) chiusura delle porte interessate immediatamente dopo la scadenza dell'accesso remoto.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.6	Garantire che i controlli di sicurezza per l'accesso remoto al server includano quanto segue: (a) limitazione dell'acce sso solo ai dispositi vi endpoint protetti e bloccati; (b) utilizzo di tunnel sicuri come TLS e VPN IPSec; (c) implementazione di un server "gateway" con difese e protezion i perimetrali adeguate come firewall, IPS e antivirus; e (d) chiusura delle porte interessate immediata mente dopo la scadenza dell'acce sso remoto.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 5.6	Garantire che i controlli di sicurezza per l'accesso remoto al server includano quanto segue: (a) limitazione dell'accesso solo ai dispositivi endpoint protetti e bloccati; (b) utilizzo di tunnel sicuri come TLS e VPN IPSec; (c) implementazione di un server "gateway" con difese e protezioni perimetrali adeguate come firewall, IPS e antivirus; e (d) chiusura delle porte interessate immediatamente dopo la scadenza dell'accesso remoto.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 1 (a)	Un istituto finanziario deve progettare un'architettura cloud solida e garantire che tale progettazione sia conforme agli standard internazionali pertinenti per l'applicazione prevista.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 1 (b)	Un istituto finanziar io è incoraggiato ad adottare i principi zero-trust per fornire un'architettura resiliente agli attacchi informatici adottando una mentalità basata sulla «presunzi one di violazion e», applicando la microsegmentazione , i diritti di accesso «deny-by-default» e «con privilegi minimi» e conducend o ispezioni defense-i n-depth approfondite e convalide continue, ove applicabile.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 1 (b)	Un istituto finanziario è incoraggiato ad adottare i principi zero-trust per fornire un'architettura resiliente agli attacchi informatici adottando una mentalità basata sulla «presunzione di violazione», applicando la microsegmentazione, i diritti di accesso «deny-by-default» e «con defense-in-depth privilegi minimi» e conducendo ispezioni approfondite e convalide continue, ove applicabile.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 1 (b)	Un istituto finanziario è incoraggiato ad adottare i principi zero-trust per fornire un'architettura resiliente dal punto di vista informatico adottando una mentalità basata sulla «presunzione di violazione», prevedendo livelli di defense-in-depth microsegmentazione, «deny-by-default», diritti di accesso con «privilegio minimo» e conducendo ispezioni approfondite e convalide continue, ove applicabile.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 1 (b)	Un istituto finanziario è incoraggiato ad adottare i principi zero-trust per fornire un'architettura resiliente agli attacchi informatici adottando una mentalità basata sulla presunzione di violazione, applicando la microsegmentazione, i diritti di accesso «deny-by-default» e «con privilegi minimi» e conducendo ispezioni defense-in-depth approfondite e convalide continue, ove applicabile.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 1 (c)	Nella gestione della complessità dell'ambiente di rete cloud, un istituto finanziario deve utilizzare l'approccio all'architettura di rete più recente e un concetto e soluzioni di progettazione di rete appropriati per gestire e monitorare la sicurezza granulare della rete e il provisioning della rete centralizzata.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 1 (c)	Nella gestione della complessità dell'ambiente di rete cloud, un istituto finanziario deve utilizzare l'approcc io all'architettura di rete più recente e un concetto e soluzioni di progettazione di rete appropriati per gestire e monitorare la sicurezza granulare della rete e il provision ing della rete centraliz zata.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
Appendice 10 parte B - 1 (d)	Un istituto finanziar io deve stabilire e utilizzare canali di comunicazione sicuri e crittografati per la migrazione di server fisici, applicazioni o dati verso le piattafor me cloud.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 1 (d)	Un istituto finanziario deve stabilire e utilizzare canali di comunicazione sicuri e crittografati per la migrazione di server fisici, applicazioni o dati verso le piattaforme cloud.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 1 (f) i)	Il maggiore utilizzo delle interfacce di programmazione delle applicazioni (API) da parte degli istituti finanziari per l'interconnessione con fornitori di servizi applicativi esterni potrebbe contribui re all'efficienza nella fornitura di nuovi servizi. Tuttavia, ciò può aumentare la superficie degli attacchi informati ci e una gestione per qualsiasi motivo errata può amplifica re l'impatto di un incidente di sicurezza delle informazioni. Un istituto finanziar io deve garantire che le proprie API siano soggette a rigorosi meccanism i di gestione e controllo, tra cui: i) le API devono essere progettate per la resilienza del servizio, al fine di	api-gwv2-authoriza tion-type-configured	È opportuno assicurar si che il proprio percorso API Amazon API Gateway v2 abbia un tipo di autorizza zione impostato per impedire l'accesso non autorizzato alle risorse di backend sottostanti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	evitare la presenza di singoli punti deboli, e configurate in modo sicuro con controlli di accesso adeguati;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 1 (f) ii)	Il maggiore utilizzo delle interfacce di programmazione delle applicazioni (API) da parte degli istituti finanziari per l'interconnessione con fornitori di servizi applicativi esterni potrebbe contribui re all'efficienza nella fornitura di nuovi servizi. Tuttavia, ciò può aumentare la superficie degli attacchi informati ci e una gestione per qualsiasi motivo errata può amplifica re l'impatto di un incidente di sicurezza delle informazioni. Un istituto finanziar io deve garantire che le proprie API siano soggette a rigorosi meccanismi di gestione e controllo , tra cui: ii) le API devono essere monitorate contro gli attacchi informati ci con adeguate	api-gw-associated-with-waf	AWS WAF consente di configurare una serie di regole (denominate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	misure di risposta agli incidenti e disattiva te tempestivamente quando non sono più in uso.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 1 (f) ii)	Il maggiore utilizzo delle interfacce di programmazione delle applicazioni (API) da parte degli istituti finanziari per l'interconnessione con fornitori di servizi applicativi esterni potrebbe contribui re all'efficienza nella fornitura di nuovi servizi. Tuttavia, ciò può aumentare la superficie degli attacchi informati ci e una gestione per qualsiasi motivo errata può amplifica re l'impatto di un incidente di sicurezza delle informazioni. Un istituto finanziar io deve garantire che le proprie API siano soggette a rigorosi meccanismi di gestione e controllo , tra cui: ii) le API devono essere monitorate contro gli attacchi informati ci con adeguate	api-gw-execution-l ogging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	misure di risposta agli incidenti e disattiva te tempestivamente quando non sono più in uso.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 2 (b) ii)	Un istituto finanziario deve sfruttare continuamente le funzionalità cloud avanzate per migliorare la sicurezza dei servizi cloud. Inoltre, tra le altre cose, gli istituti finanziari sono incoraggiati a: ii) utilizzare pratiche infrastrutturali immutabili per l'implementazione dei servizi e creare un nuovo ambiente con l'ultima versione stabile del software per ridurre il rischio di errori. Il monitoraggio continuo dell'ambiente cloud deve includere l'automazione del rilevamento delle modifiche all'infrastruttura immutabile per migliorare la revisione della conformità e combattere gli attacchi informatici in continua evoluzione	cloudformation-stack-notification-check	Per rilevare modifiche non intenzionali alle AWS risorse sottostanti, assicurati che lo CloudFormation stack sia configurato per inviare notifiche di eventi a un argomento Amazon SNS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 3 (b) vi)	Un istituto finanziario deve garantire che le immagini delle macchine virtuali e dei container siano configurate, rafforzate e monitorate in modo appropriato. Ciò include quanto segue: vi) le immagini archiviate sono soggette a monitoraggio di sicurezza in caso di accessi e modifiche non autorizzati.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (a) i)	Nell'ambito di un'efficace capacità di ripristino, gli istituti finanziari devono garantire che le procedure di backup e ripristino esistenti siano estese ai servizi cloud, il che include quanto segue: i) definire e formalizzare la strategia di backup e ripristino nella fase di pianificazione dell'adozione del cloud;	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (a) i)	Nell'ambito di un'efficace capacità di ripristino, gli istituti finanziari devono garantire che le procedure di backup e ripristino esistenti siano estese ai servizi cloud, il che include quanto segue: i) definire e formalizzare la strategia di backup e ripristino nella fase di pianificazione dell'adozione del cloud;	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (a) i)	Nell'ambito di un'efficace capacità di ripristino, gli istituti finanziari devono garantire che le procedure di backup e ripristino esistenti siano estese ai servizi cloud, il che include quanto segue: i) definire e formalizzare la strategia di backup e ripristino nella fase di pianificazione dell'adozione del cloud;	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (a) i)	Nell'ambito di un'efficace capacità di ripristino, gli istituti finanziari devono garantire che le procedure di backup e ripristino esistenti siano estese ai servizi cloud, il che include quanto segue: i) definire e formalizzare la strategia di backup e ripristino nella fase di pianificazione dell'adozione del cloud;	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (a) i)	Nell'ambito di un'efficace capacità di ripristino, gli istituti finanziari devono garantire che le procedure di backup e ripristino esistenti siano estese ai servizi cloud, il che include quanto segue: i) definire e formalizzare la strategia di backup e ripristino nella fase di pianificazione dell'adozione del cloud;	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (a) i)	Nell'ambito di un'efficace capacità di ripristino, gli istituti finanziari devono garantire che le procedure di backup e ripristino esistenti siano estese ai servizi cloud, il che include quanto segue: i) definire e formalizzare la strategia di backup e ripristino nella fase di pianificazione dell'adozione del cloud;	s3-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i bucket Amazon Simple Storage Service (S3) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 5 (b)	Un istituto finanziario deve garantire che le procedure di backup e ripristino siano testate periodica mente per convalidare le capacità di ripristin o. La frequenza delle procedure di backup deve essere commisurata alla criticità del sistema e all'obiettivo del punto di ripristino (RPO) del sistema. L'istitut o finanziario deve adottare tempestiv amente le azioni correttive in caso di backup non riusciti.	backup-plan-min-fr equency-and-min-re tention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservaz ione minime. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredF requencyValue (Config default: 1), (requiredRetentionD ays Config default: 35) e (requiredF requencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (c) i)	Un istituto finanziario dovrebbe garantire un backup e un ripristino sufficienti della macchina virtuale e del contenitore, comprese le impostazioni di configurazione del backup (per IaaS e PaaS, se del caso), che includono quanto segue: i) garantire la capacità di ripristinare una macchina virtuale e un contenitore secondo point-in-time quanto specificato dagli obiettivi di ripristino aziendali;	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (d) i)	Un istituto finanziario deve valutare i requisiti di resilienza dei servizi cloud e individuare misure appropriate commisurate alla criticità del sistema, per garantire la disponibilità del servizio in scenari estremamente avversi. Gli istituti finanziari devono prendere in considerazione un approccio basato sul rischio e adottare progressivamente controlli di mitigazione adeguati per garantire la disponibilità dei servizi e diminuire il rischio di concentrazione. Tra le opzioni praticabili vi sono: i) sfruttare le funzionalità di elevata disponibilità e ridondanza dei servizi cloud per garantire che data center di produzione abbiano capacità ridondant	autoscaling-multiple-az	Per garantire un'elevata disponibilità, assicurati che il gruppo Auto Scaling sia configurato su più zone di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e in diverse zone di disponibilità;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (d) i)	Un istituto finanziario deve valutare i requisiti di resilienza dei servizi cloud e individuare misure appropriate commisurate alla criticità del sistema, per garantire la disponibilità del servizio in scenari estremamente avversi. Gli istituti finanziari devono prendere in considerazione un approccio basato sul rischio e adottare progressivamente controlli di mitigazione adeguati per garantire la disponibilità dei servizi e diminuire il rischio di concentrazione. Tra le opzioni praticabili vi sono: i) sfruttare le funzionalità di elevata disponibilità e ridondanza dei servizi cloud per garantire che data center di produzione abbiano capacità ridondant	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurati che ELB abbia registrato istanze da più zone di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e in diverse zone di disponibilità;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (d) i)	Un istituto finanziario deve valutare i requisiti di resilienza dei servizi cloud e individuare misure appropriate commisurate alla criticità del sistema, per garantire la disponibilità del servizio in scenari estremamente avversi. Gli istituti finanziari devono prendere in considerazione un approccio basato sul rischio e adottare progressivamente controlli di mitigazione adeguati per garantire la disponibilità dei servizi e diminuire il rischio di concentrazione. Tra le opzioni praticabili vi sono: i) sfruttare le funzionalità di elevata disponibilità e ridondanza dei servizi cloud per garantire che data center di produzione abbiano capacità ridondant	lambda-vpc-multi-az-check	Se la tua funzione AWS Lambda è configurata per la connessione a un cloud privato virtuale (VPC) nel tuo account, implementa la funzione AWS Lambda in almeno due zone di disponibilità diverse per assicurarti che sia disponibile per elaborare gli eventi in caso di interruzione del servizio in una singola zona.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e in diverse zone di disponibilità;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (d) i)	Un istituto finanziario deve valutare i requisiti di resilienza dei servizi cloud e individuare misure appropriate commisurate alla criticità del sistema, per garantire la disponibilità del servizio in scenari estremamente avversi. Gli istituti finanziari devono prendere in considerazione un approccio basato sul rischio e adottare progressivamente controlli di mitigazione adeguati per garantire la disponibilità dei servizi e diminuire il rischio di concentrazione. Tra le opzioni praticabili vi sono: i) sfruttare le funzionalità di elevata disponibilità e ridondanza dei servizi cloud per garantire che data center di produzione abbiano capacità ridondant	nlb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per i tuoi sistemi di bilanciamento (NetworkLoad NLB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e in diverse zone di disponibilità;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (d) i)	Un istituto finanziario deve valutare i requisiti di resilienza dei servizi cloud e individuare misure appropriate commisurate alla criticità del sistema, per garantire la disponibilità del servizio in scenari estremamente avversi. Gli istituti finanziari devono prendere in considerazione un approccio basato sul rischio e adottare progressivamente controlli di mitigazione adeguati per garantire la disponibilità dei servizi e diminuire il rischio di concentrazione. Tra le opzioni praticabili vi sono: i) sfruttare le funzionalità di elevata disponibilità e ridondanza dei servizi cloud per garantire che data center di produzione abbiano capacità ridondant	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relational Database Service (Amazon RDS). Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e in diverse zone di disponibilità;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 5 (d) i)	Un istituto finanziario deve valutare i requisiti di resilienza dei servizi cloud e individuare misure appropriate commisurate alla criticità del sistema, per garantire la disponibilità del servizio in scenari estremamente avversi. Gli istituti finanziari devono prendere in considerazione un approccio basato sul rischio e adottare progressivamente controlli di mitigazione adeguati per garantire la disponibilità dei servizi e diminuire il rischio di concentrazione. Tra le opzioni praticabili vi sono: i) sfruttare le funzionalità di elevata disponibilità e ridondanza dei servizi cloud per garantire che data center di produzione abbiano capacità ridondant	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e in diverse zone di disponibilità;		e le operazioni del database non appena il failover è completato.
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	eks-secrets-encrypted	Per proteggere i dati a riposo, assicurati che i cluster Amazon Elastic Kubernetes Service (EKS) siano configurati per abilitare la crittografia dei segreti Kubernetes. Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 8 (a)	Un istituto finanziario deve implementare tecniche di crittografia appropriate e pertinenti per proteggere la riservatezza e l'integrità dei dati sensibili archiviati nel cloud.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 8 (d)	Con la maggiore adozione del cloud, la gestione di molte chiavi di crittografia utilizzate per proteggere i dati è diventata più complessa e può porre gli istituti finanziari di fronte a nuove sfide. Un istituto finanziario deve adottare un approccio di gestione delle chiavi completo e centralizzato, che include l'uso di un sistema di gestione delle chiavi centralizzato in grado di gestire generazioni, archiviazione e distribuzione delle chiavi in modo sicuro e dimensionabile.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 8 (d)	Con la maggiore adozione del cloud, la gestione di molte chiavi di crittografia utilizzate per proteggere i dati è diventata più complessa e può porre gli istituti finanziari di fronte a nuove sfide. Un istituto finanziario deve adottare un approccio di gestione delle chiavi completo e centralizzato, che include l'uso di un sistema di gestione delle chiavi centralizzato in grado di gestire generazioni, archiviazione e distribuzione delle chiavi in modo sicuro e dimensionabile.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 9 (a) ii)	Il piano di gestione costituisce una differenza fondamentale in termini di sicurezza tra l'infrastruttura tradizionale e il cloud computing, dove l'accesso remoto è supportato per impostazione predefinita. Questo livello di accesso potrebbe aprire la strada ad attacchi informatici e mettere così a rischio l'integrità dell'intera implementazione del cloud. In considerazione di ciò, gli istituti finanziari dovrebbero garantire l'uso di controlli rigorosi per l'accesso al piano di gestione, che possono includere quanto segue: ii) implementare il «privilegio minimo» e l'autenticazione forte a più fattori (MFA), ad esempio password complesse, soft token,	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundatio

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	strumento di gestione degli accessi privilegi ati e funzioni maker-checker;		nal Security Best Practices value: true), MinimumPa sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24) e MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 9 (a) ii)	Il piano di gestione costituisce una differenza fondamentale in termini di sicurezza tra l'infrastruttura tradizionale e il cloud computing, dove l'accesso remoto è supportato o per impostazione predefinita. Questo livello di accesso potrebbe aprire la strada ad attacchi informatici e mettere così a rischio l'integrità dell'intera implementazione del cloud. In considerazione di ciò, gli istituti finanziari dovrebbero garantire l'uso di controlli rigorosi per l'accesso al piano di gestione, che possono includere quanto segue: ii) implementare il «privilegio minimo» e l'autenticazione forte a più fattori (MFA), ad esempio password complesse, soft token,	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel Cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti IAM. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti di account compromessi richiedendo l'autenticazione a più fattori per gli utenti IAM.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	strumento di gestione degli accessi privilegi ati e funzioni maker-checker;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 9 (a) ii)	Il piano di gestione costituisce una differenza fondamentale in termini di sicurezza tra l'infrastruttura tradizionale e il cloud computing, dove l'accesso remoto è supportato per impostazione predefinita. Questo livello di accesso potrebbe aprire la strada ad attacchi informatici e mettere così a rischio l'integrità dell'intera implementazione del cloud. In considerazione di ciò, gli istituti finanziari dovrebbero garantire l'uso di controlli rigorosi per l'accesso al piano di gestione, che possono includere quanto segue: ii) implementare il «privilegio minimo» e l'autenticazione forte a più fattori (MFA), ad esempio password complesse, soft token,	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	strumento di gestione degli accessi privilegi ati e funzioni maker-checker;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 9 (a) ii)	Il piano di gestione costituisce una differenza fondamentale in termini di sicurezza tra l'infrastruttura tradizionale e il cloud computing, dove l'accesso remoto è supportato per impostazione predefinita. Questo livello di accesso potrebbe aprire la strada ad attacchi informatici e mettere così a rischio l'integrità dell'intera implementazione del cloud. In considerazione di ciò, gli istituti finanziari dovrebbero garantire l'uso di controlli rigorosi per l'accesso al piano di gestione, che possono includere quanto segue: ii) implementare il «privilegio minimo» e l'autenticazione forte a più fattori (MFA), ad esempio password complesse, soft token,	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	strumento di gestione degli accessi privilegi ati e funzioni maker-checker;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 9 (a) iii)	Il piano di gestione costituisce una differenza fondamentale in termini di sicurezza tra l'infrastruttura tradizionale e il cloud computing, dove l'accesso remoto è supportato o per impostazione predefinita. Questo livello di accesso potrebbe aprire la strada ad attacchi informatici e mettere così a rischio l'integrità dell'intera implementazione del cloud. In considerazione di ciò, gli istituti finanziari devono garantire l'applicazione di controlli rigorosi per l'accesso al piano di gestione, che possono includere quanto segue: iii) assegnazione granulare dei diritti per gli utenti privilegiati;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 9 (a) iii)	Il piano di gestione costituisce una differenza fondamentale in termini di sicurezza tra l'infrastruttura tradizionale e il cloud computing, dove l'accesso remoto è supportato o per impostazione predefinita. Questo livello di accesso potrebbe aprire la strada ad attacchi informatici e mettere così a rischio l'integrità dell'intera implementazione del cloud. In considerazione di ciò, gli istituti finanziari devono garantire l'applicazione di controlli rigorosi per l'accesso al piano di gestione, che possono includere quanto segue: iii) assegnazione granulare dei diritti per gli utenti privilegiati;	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 9 (a) iv)	Il piano di gestione costituisce una differenza fondamentale in termini di sicurezza tra l'infrastruttura tradizionale e il cloud computing, dove l'accesso remoto è supportato o per impostazione predefinita. Questo livello di accesso potrebbe aprire la strada ad attacchi informatici e mettere così a rischio l'integrità dell'intera implementazione del cloud. In considerazione di ciò, gli istituti finanziari devono garantire l'applicazione di controlli rigorosi per l'accesso al piano di gestione, che possono includere quanto segue: iv) monitoraggio continuo delle attività svolte dagli utenti privilegiati;	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 9 (a) iv)	Il piano di gestione costituisce una differenza fondamentale in termini di sicurezza tra l'infrastruttura tradizionale e il cloud computing, dove l'accesso remoto è supportato o per impostazione predefinita. Questo livello di accesso potrebbe aprire la strada ad attacchi informatici e mettere così a rischio l'integrità dell'intera implementazione del cloud. In considerazione di ciò, gli istituti finanziari devono garantire l'applicazione di controlli rigorosi per l'accesso al piano di gestione, che possono includere quanto segue: iv) monitoraggio continuo delle attività svolte dagli utenti privilegiati;	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 12 (a)	Un istituto finanziario deve proteggere i dati ospitati nei servizi cloud come richiesto nella sezione Prevenzione della perdita di dati (paragrafi da 11.14 a 11.16) del presente documento di policy, il che include l'espansione dell'impronta degli endpoint se l'istituto finanziario consente al personale di utilizzare i propri dispositivi per accedere ai dati sensibili.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10 parte B - 12 (a)	Un istituto finanziario deve proteggere i dati ospitati nei servizi cloud come richiesto nella sezione Prevenzione della perdita di dati (paragrafi da 11.14 a 11.16) del presente documento di policy, il che include l'espansione dell'impronta degli endpoint se l'istituto finanziario consente al personale di utilizzare i propri dispositivi per accedere ai dati sensibili.	macie-status-check	Amazon Macie è un servizio di sicurezza dei dati che utilizza il machine learning (ML) e la corrispondenza di modelli per individuare e aiutare a proteggere i dati sensibili archiviati in Amazon Simple Storage Service (Amazon S3).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 14 (c) i)	Un istituto finanziario deve prendere in considerazione le seguenti misure aggiuntive nello sviluppo del proprio CIRP: i) migliorare la propria capacità di individuare gli incidenti di violazione della sicurezza per conseguire una gestione degli incidenti efficace, che includa la capacità di rilevare la fuga di dati sul dark web;	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Appendice 10, parte B - 14 (c) i)	Un istituto finanziario deve prendere in considerazione le seguenti misure aggiuntive nello sviluppo del proprio CIRP: i) migliorare la propria capacità di individuare gli incidenti di violazione della sicurezza per conseguire una gestione degli incidenti efficace, che includa la capacità di rilevare la fuga di dati sul dark web;	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for BNM RMit.

Best practice operative per il Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il Medium Cloud Control Profile del Canadian Centre for Cyber Security (CCCS) e le regole AWS Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CCCS Medium Cloud Control Profile. Un controllo del profilo CCCS Medium Cloud Control può fare riferimento a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			CloudTrail Record Contents.
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(1)	AC-2(1) Gestione degli account | Gestione automatizzata degli account di sistema	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(3)	AC-2(3) Gestione dell'account | Disabilitazione degli account inattivi	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(3)	AC-2(3) Gestione dell'account | Disabilitazione degli account inattivi	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(4)	AC-2(4) Gestione degli account | Azioni di audit automatizzate	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
CCCS-fPBMM-AC-2(4)	AC-2(4) Gestione degli account | Azioni di audit automatizzate	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(4)	AC-2(4) Gestione degli account | Azioni di audit automatizzate	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(4)	AC-2(4) Gestione degli account | Azioni di audit automatizzate	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(4)	AC-2(4) Gestione degli account | Azioni di audit automatizzate	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(4)	AC-2(4) Gestione degli account | Azioni di audit automatizzate	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2(4)	AC-2(4) Gestione degli account | Azioni di audit automatizzate	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registran do le azioni della Console di gestione e le chiamate API. AWS È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.A	AC-2.A Gestione degli account	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.B	AC-2.B Gestione degli account	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.C	AC-2.C Gestione degli account	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.D	AC-2.D Gestione degli account	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.E	AC-2.E Gestione degli account	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.F	AC-2.F Gestione degli account	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.G	AC-2.G Gestione degli account	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.H	AC-2.H Gestione degli account	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.I	AC-2.I Gestione degli account	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.J	AC-2.J Gestione degli account	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-2.K	AC-2.K Gestione degli account	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-3.A	AC-3.A Applicazione degli accessi	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
CCCS-fPBMM-AC-4(21)	AC-4(21) Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4(21)	AC-4(21) Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
CCCS-fPBMM-AC-4(21)	AC-4(21) Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4(21)	AC-4(21) Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4(21)	AC-4(21) Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
CCCS-fPBMM-AC-4(21)	AC-4(21) Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4(21)	AC-4(21) Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-AC-4(21)	AC-4(21) Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4(21)	AC-4(21) Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-4.A	AC-4.A Applicazione del flusso di informazioni	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-5.A	AC-5.A Separazione dei compiti	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-5.A	AC-5.A Separazione dei compiti	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-5.A	AC-5.A Separazione dei compiti	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-5.A	AC-5.A Separazione dei compiti	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-5.A	AC-5.A Separazione dei compiti	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(1)	AC-6(1) Privilegio minimo | Autorizzazione dell'accesso alle funzioni di sicurezza	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(1)	AC-6(1) Privilegio minimo | Autorizzazione dell'accesso alle funzioni di sicurezza	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(1)	AC-6(1) Privilegio minimo | Autorizzazione dell'accesso alle funzioni di sicurezza	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(1)	AC-6(1) Privilegio minimo | Autorizzazione dell'accesso alle funzioni di sicurezza	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(1)	AC-6(1) Privilegio minimo | Autorizzazione dell'accesso alle funzioni di sicurezza	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(2)	AC-6(2) Privilegio minimo | Accesso senza privilegi per funzioni non legate alla sicurezza	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(2)	AC-6(2) Privilegio minimo | Accesso senza privilegi per funzioni non legate alla sicurezza	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(2)	AC-6(2) Privilegio minimo | Accesso senza privilegi per funzioni non legate alla sicurezza	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(2)	AC-6(2) Privilegio minimo | Accesso senza privilegi per funzioni non legate alla sicurezza	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(2)	AC-6(2) Privilegio minimo | Accesso senza privilegi per funzioni non legate alla sicurezza	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(5)	AC-6(5) Privilegio minimo | Account con privilegi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(5)	AC-6(5) Privilegio minimo | Account con privilegi	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(5)	AC-6(5) Privilegio minimo | Account con privilegi	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(5)	AC-6(5) Privilegio minimo | Account con privilegi	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio minimo | Audit dell'utilizzo delle funzioni con privilegi	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio minimo | Audit dell'utilizzo delle funzioni con privilegi	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio minimo | Audit dell'utilizzo delle funzioni con privilegi	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio minimo | Audit dell'utilizzo delle funzioni con privilegi	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio minimo | Audit dell'utilizzo delle funzioni con privilegi	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio minimo | Audit dell'utilizzo delle funzioni con privilegi	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(9)	AC-6(9) Privilegio minimo | Audit dell'utilizzo delle funzioni con privilegi	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(10)	AC-6(10) Privilegio minimo | Divieto per gli utenti senza privilegi di eseguire funzioni con privilegi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(10)	AC-6(10) Privilegi o minimo | Divieto per gli utenti senza privilegi di eseguire funzioni con privilegi	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(10)	AC-6(10) Privilegi o minimo | Divieto per gli utenti senza privilegi di eseguire funzioni con privilegi	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(10)	AC-6(10) Privilegi o minimo | Divieto per gli utenti senza privilegi di eseguire funzioni con privilegi	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6(10)	AC-6(10) Privilegio minimo | Divieto per gli utenti senza privilegi di eseguire funzioni con privilegi	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-6.A	AC-6.A Privilegio minimo	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(1)	AC-17(1) Accesso remoto | Monitoraggio/controllo automatizzati	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(2)	AC-17(2) Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-AC-17(2)	AC-17(2) Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(2)	AC-17(2) Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(2)	AC-17(2) Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
CCCS-fPBMM-AC-17(2)	AC-17(2) Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-AC-17(2)	AC-17(2) Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(3)	AC-17(3) Accesso remoto | Punti di controllo degli accessi gestiti	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(4)	AC-17(4) Accesso remoto | Comandi/accesso con privilegi	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(4)	AC-17(4) Accesso remoto | Comandi/accesso con privilegi	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17(4)	AC-17(4) Accesso remoto | Comandi/accesso con privilegi	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.A	AC-17.A Accesso remoto	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.AA	AC-17.AA Accesso remoto	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AC-17.B	AC-17.B Accesso remoto	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.A	AU-2.A eventi di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
CCCS-fPBMM-AU-2.A	AU-2.A eventi di audit	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.A	AU-2.A eventi di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CCCS-fPBMM-AU-2.A	AU-2.A eventi di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.A	AU-2.A eventi di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.A	AU-2.A eventi di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.A	AU-2.A eventi di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.A	AU-2.A eventi di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.A	AU-2.A eventi di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.A	AU-2.A eventi di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.A	AU-2.A eventi di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
CCCS-fPBMM-AU-2.B	AU-2.B Eventi di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.B	AU-2.B Eventi di audit	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
CCCS-fPBMM-AU-2.B	AU-2.B Eventi di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.B	AU-2.B Eventi di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.B	AU-2.B Eventi di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.B	AU-2.B Eventi di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.B	AU-2.B Eventi di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.B	AU-2.B Eventi di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.B	AU-2.B Eventi di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.B	AU-2.B Eventi di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.B	AU-2.B Eventi di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
CCCS-fPBMM-AU-2.C	AU-2.C Eventi di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.C	AU-2.C Eventi di audit	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
CCCS-fPBMM-AU-2.C	AU-2.C Eventi di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.C	AU-2.C Eventi di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.C	AU-2.C Eventi di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.C	AU-2.C Eventi di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.C	AU-2.C Eventi di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.C	AU-2.C Eventi di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.C	AU-2.C Eventi di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.C	AU-2.C Eventi di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.C	AU-2.C Eventi di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
CCCS-fPBMM-AU-2.D	AU-2.D Eventi di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.D	AU-2.D Eventi di audit	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
CCCS-fPBMM-AU-2.D	AU-2.D Eventi di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.D	AU-2.D Eventi di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.D	AU-2.D Eventi di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.D	AU-2.D Eventi di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.D	AU-2.D Eventi di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.D	AU-2.D Eventi di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.D	AU-2.D Eventi di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.D	AU-2.D Eventi di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-2.D	AU-2.D Eventi di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenuto dei record di audit | Informazioni di audit aggiuntive	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenuto dei record di audit | Informazioni di audit aggiuntive	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenuto dei record di audit | Informazioni di audit aggiuntive	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenuto dei record di audit | Informazioni di audit aggiuntive	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenuto dei record di audit | Informazioni di audit aggiuntive	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenuto dei record di audit | Informazioni di audit aggiuntive	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenuto dei record di audit | Informazioni di audit aggiuntive	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3(1)	AU-3(1) Contenuto dei record di audit | Informazioni di audit aggiuntive	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-3.A	AU-3.A Contenuto dei record di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-5.A	AU-5.A Risposta agli errori di elaborazione degli audit	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-5.B	AU-5.B Risposta agli errori di elaborazione degli audit	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(1)	AU-6(1) Revisione , analisi e reporting degli audit | Integrazione dei processi	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(1)	AU-6(1) Revisione , analisi e reporting degli audit | Integrazione dei processi	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
CCCS-fPBMM-AU-6(1)	AU-6(1) Revisione , analisi e reporting degli audit | Integrazione dei processi	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(1)	AU-6(1) Revisione , analisi e reporting degli audit | Integrazione dei processi	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(1)	AU-6(1) Revisione , analisi e reporting degli audit | Integrazione dei processi	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(1)	AU-6(1) Revisione , analisi e reporting degli audit | Integrazione dei processi	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail log. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-6(3)	AU-6(3) Revisione , analisi e reporting degli audit | Correlazione dei repository di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-7(1)	AU-7(1) Riduzione dei record di audit e generazione di report | Elaborazione automatica	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	api-gw-execution-l ogging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-8.B	AU-8.B Timestamp	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-9(2)	AU-9(2) Protezione delle informazioni di audit | Backup degli audit su sistemi o componenti fisici separati	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CCCS-fPBMM-AU-9(2)	AU-9(2) Protezion e delle informazioni di audit | Backup degli audit su sistemi o componenti fisici separati	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-9(2)	AU-9(2) Protezione delle informazioni di audit | Backup degli audit su sistemi o componenti fisici separati	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.
CCCS-fPBMM-AU-9.A	AU-9.A Protezione delle informazioni di audit	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-9.A	AU-9.A Protezione delle informazioni di audit	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-9.A	AU-9.A Protezione delle informazioni di audit	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
CCCS-fPBMM-AU-11.A	AU-11.A Conservazione dei record di audit	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-11.B	AU-11.B Conservazione dei record di audit	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.
CCCS-fPBMM-AU-11.C	AU-11.C Conservazione dei record di audit	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.A	AU-12.A Generazione di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
CCCS-fPBMM-AU-12.C	AU-12.C Generazione di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.C	AU-12.C Generazione di audit	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
CCCS-fPBMM-AU-12.C	AU-12.C Generazione di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.C	AU-12.C Generazione di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.C	AU-12.C Generazione di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.C	AU-12.C Generazione di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.C	AU-12.C Generazione di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.C	AU-12.C Generazione di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.C	AU-12.C Generazione di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.C	AU-12.C Generazione di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-AU-12.C	AU-12.C Generazione di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-3(5)	CA-3(5) Interconnessioni di sistemi | Limitazioni per connessioni di rete esterne	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	api-gw-xray-enabled	AWS X-Ray raccoglie dati sulle richieste servite dall'applicazione e fornisce strumenti che è possibile utilizzare per visualizzare, filtrare e acquisire informazioni su tali dati per identificare problemi e opportunità di ottimizzazione. Assicurati che X-Ray sia abilitato in modo da poter visualizzare informazioni dettagliate non solo sulla richiesta e sulla risposta, ma anche sulle chiamate effettuate dall'applicazione a AWS risorse downstream, microservizi, database e API Web HTTP.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.A	CA-7.A Monitoraggio continuo	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	api-gw-xray-enabled	AWS X-Ray raccoglie dati sulle richieste servite dall'appl icazione e fornisce strumenti che è possibile utilizzar e per visualizzare, filtrare e acquisire informazioni su tali dati per identificare problemi e opportuni tà di ottimizzazione. Assicurati che X-Ray sia abilitato in modo da poter visualizzare informazi oni dettagliate non solo sulla richiesta e sulla risposta, ma anche sulle chiamate effettuate dall'appl icazione a AWS risorse downstream, microservizi, database e API Web HTTP.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.B	CA-7.B Monitoraggio continuo	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	api-gw-xray-enabled	AWS X-Ray raccoglie dati sulle richieste servite dall'appl icazione e fornisce strumenti che è possibile utilizzar e per visualizzare, filtrare e acquisire informazioni su tali dati per identificare problemi e opportuni tà di ottimizzazione. Assicurati che X-Ray sia abilitato in modo da poter visualizzare informazi oni dettagliate non solo sulla richiesta e sulla risposta, ma anche sulle chiamate effettuate dall'appl icazione a AWS risorse downstream, microservizi, database e API Web HTTP.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.C	CA-7.C Monitoraggio continuo	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	api-gw-xray-enabled	AWS X-Ray raccoglie dati sulle richieste servite dall'appl icazione e fornisce strumenti che è possibile utilizzar e per visualizzare, filtrare e acquisire informazioni su tali dati per identificare problemi e opportuni tà di ottimizzazione. Assicurati che X-Ray sia abilitato in modo da poter visualizzare informazi oni dettagliate non solo sulla richiesta e sulla risposta, ma anche sulle chiamate effettuate dall'appl icazione a AWS risorse downstream, microservizi, database e API Web HTTP.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.D	CA-7.D Monitoraggio continuo	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	api-gw-xray-enabled	AWS X-Ray raccoglie dati sulle richieste servite dall'applicazione e fornisce strumenti che è possibile utilizzare per visualizzare, filtrare e acquisire informazioni su tali dati per identificare problemi e opportunità di ottimizzazione. Assicurati che X-Ray sia abilitato in modo da poter visualizzare informazioni dettagliate non solo sulla richiesta e sulla risposta, ma anche sulle chiamate effettuate dall'applicazione a AWS risorse downstream, microservizi, database e API Web HTTP.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.E	CA-7.E Monitoraggio continuo	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	api-gw-xray-enabled	AWS X-Ray raccoglie dati sulle richieste servite dall'appl icazione e fornisce strumenti che è possibile utilizzar e per visualizzare, filtrare e acquisire informazioni su tali dati per identificare problemi e opportuni tà di ottimizzazione. Assicurati che X-Ray sia abilitato in modo da poter visualizzare informazi oni dettagliate non solo sulla richiesta e sulla risposta, ma anche sulle chiamate effettuate dall'appl icazione a AWS risorse downstream, microservizi, database e API Web HTTP.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.F	CA-7.F Monitoraggio continuo	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	api-gw-xray-enabled	AWS X-Ray raccoglie dati sulle richieste servite dall'appl icazione e fornisce strumenti che è possibile utilizzar e per visualizzare, filtrare e acquisire informazioni su tali dati per identificare problemi e opportuni tà di ottimizzazione. Assicurati che X-Ray sia abilitato in modo da poter visualizzare informazi oni dettagliate non solo sulla richiesta e sulla risposta, ma anche sulle chiamate effettuate dall'appl icazione a AWS risorse downstream, microservizi, database e API Web HTTP.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-7.G	CA-7.G Monitoraggio continuo	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CA-9.A	CA-9.A Connessioni interne al sistema	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-2.A	Configurazione di base CM-2.A	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-2.A	Configurazione di base CM-2.A	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-2.A	Configurazione di base CM-2.A	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-2.A	Configurazione di base CM-2.A	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-2.A	Configurazione di base CM-2.A	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-2.A	Configurazione di base CM-2.A	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-2.A	Configurazione di base CM-2.A	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.A	CM-3.A Controllo delle modifiche alla configurazione	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.A	CM-3.A Controllo delle modifiche alla configurazione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.B	CM-3.B Controllo delle modifiche alla configurazione	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.B	CM-3.B Controllo delle modifiche alla configurazione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.C	CM-3.C Controllo delle modifiche alla configurazione	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.C	CM-3.C Controllo delle modifiche alla configurazione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.D	CM-3.D Controllo delle modifiche alla configurazione	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.D	CM-3.D Controllo delle modifiche alla configurazione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.E	CM-3.E Controllo delle modifiche alla configurazione	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.E	CM-3.E Controllo delle modifiche alla configurazione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.F	CM-3.F Controllo delle modifiche alla configurazione	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.F	CM-3.F Controllo delle modifiche alla configurazione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.G	CM-3.G Controllo delle modifiche alla configurazione	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-3.G	CM-3.G Controllo delle modifiche alla configurazione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail log. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(1)	CM-5(1) Limitazioni di accesso per modifiche | Applicazione/audit automatizzati degli accessi	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5(5)	CM-5(5) Limitazioni di accesso per modifiche | Limitazione della produzione/privilegi operativi	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-5.A	CM-5.A Limitazioni di accesso per modifiche	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6(1)	CM-6(1) Impostazioni della configurazione | Gestione centrale automatizzata / Applicazione / Verifica	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6(1)	CM-6(1) Impostazioni della configurazione | Gestione centrale automatizzata / Applicazione / Verifica	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6(1)	CM-6(1) Impostazioni della configurazione | Gestione centrale automatizzata / Applicazione / Verifica	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.A	CM-6.A Impostazioni della configurazione	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.B	CM-6.B Impostazioni della configurazione	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.C	CM-6.C Impostazioni della configurazione	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-6.D	CM-6.D Impostazioni della configurazione	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-7.A	CM-7.A Funzionalità minima	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-7.A	CM-7.A Funzionalità minima	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-7.B	CM-7.B Funzionalità minima	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-7.B	CM-7.B Funzionalità minima	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8(1)	CM-8(1) Inventario dei componenti del sistema informativo | Aggiornamenti durante l'installazione e la rimozione	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8(1)	CM-8(1) Inventario dei componenti del sistema informativo | Aggiornamenti durante l'installazione e la rimozione	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8(2)	CM-8(2) Inventario dei componenti del sistema informativo | Manutenzione automatizzata	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8(2)	CM-8(2) Inventario dei componenti del sistema informativo | Manutenzione automatizzata	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8(3)	CM-8(3) Inventario dei componenti del sistema informativo | Rilevamento automatico dei componenti non autorizzati	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8(3)	CM-8(3) Inventario dei componenti del sistema informativo | Rilevamento automatico dei componenti non autorizzati	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8(3)	CM-8(3) Inventario dei componenti del sistema informativo | Rilevamento automatico dei componenti non autorizzati	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8(3)	CM-8(3) Inventario dei componenti del sistema informativo | Rilevamento automatico dei componenti non autorizzati	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8.A	CM-8.A Inventario dei componenti del sistema informativo	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8.A	CM-8.A Inventario dei componenti del sistema informativo	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8.B	CM-8.B Inventario dei componenti del sistema informativo	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8.B	CM-8.B Inventario dei componenti del sistema informativo	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8.C	CM-8.C Inventario dei componenti del sistema informativo	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8.C	CM-8.C Inventario dei componenti del sistema informativo	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8.D	CM-8.D Inventario dei componenti del sistema informativo	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8.D	CM-8.D Inventario dei componenti del sistema informativo	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8.E	CM-8.E Inventario dei componenti del sistema informativo	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CM-8.E	CM-8.E Inventario dei componenti del sistema informativo	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relational Database Service (Amazon RDS). Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(5)	CP-2(5) Piano di emergenza | Continuazione di missioni/funzioni aziendali essenziali	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(6)	CP-2(6) Piano di emergenza | Sito di elaborazione/storage alternativo	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(6)	CP-2(6) Piano di emergenza | Sito di elaborazione/storage alternativo	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(6)	CP-2(6) Piano di emergenza | Sito di elaborazione/storage alternativo	multi-region-cloudtrail-enabled	AWS CloudTrai l registra AWS le azioni della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(6)	CP-2(6) Piano di emergenza | Sito di elaborazione/storage alternativo	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relationa l Database Service (Amazon RDS). Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender e le operazioni del database non appena il failover è completat o.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2(6)	CP-2(6) Piano di emergenza | Sito di elaborazione/storage alternativo	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CCCS-fPBMM-CP-2(6)	CP-2(6) Piano di emergenza | Sito di elaborazione/storage alternativo	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.A	CP-2.A Piano di emergenza	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.A	CP-2.A Piano di emergenza	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.A	CP-2.A Piano di emergenza	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.A	CP-2.A Piano di emergenza	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.A	CP-2.A Piano di emergenza	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relationa l Database Service (Amazon RDS). Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender e le operazioni del database non appena il failover è completat o.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.A	CP-2.A Piano di emergenza	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.A	CP-2.A Piano di emergenza	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CCCS-fPBMM-CP-2.A	CP-2.A Piano di emergenza	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.B	CP-2.B Piano di emergenza	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.B	CP-2.B Piano di emergenza	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.B	CP-2.B Piano di emergenza	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.B	CP-2.B Piano di emergenza	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.B	CP-2.B Piano di emergenza	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relationa l Database Service (Amazon RDS). Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender e le operazioni del database non appena il failover è completat o.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.B	CP-2.B Piano di emergenza	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.B	CP-2.B Piano di emergenza	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CCCS-fPBMM-CP-2.B	CP-2.B Piano di emergenza	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.C	CP-2.C Piano di emergenza	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.C	CP-2.C Piano di emergenza	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.C	CP-2.C Piano di emergenza	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.C	CP-2.C Piano di emergenza	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.C	CP-2.C Piano di emergenza	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relationa l Database Service (Amazon RDS). Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender e le operazioni del database non appena il failover è completat o.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.C	CP-2.C Piano di emergenza	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.C	CP-2.C Piano di emergenza	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CCCS-fPBMM-CP-2.C	CP-2.C Piano di emergenza	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.D	CP-2.D Piano di emergenza	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.D	CP-2.D Piano di emergenza	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.D	CP-2.D Piano di emergenza	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.D	CP-2.D Piano di emergenza	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.D	CP-2.D Piano di emergenza	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relationa l Database Service (Amazon RDS). Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender e le operazioni del database non appena il failover è completat o.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.D	CP-2.D Piano di emergenza	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.D	CP-2.D Piano di emergenza	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CCCS-fPBMM-CP-2.D	CP-2.D Piano di emergenza	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.E	CP-2.E Piano di emergenza	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.E	CP-2.E Piano di emergenza	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.E	CP-2.E Piano di emergenza	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.E	CP-2.E Piano di emergenza	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.E	CP-2.E Piano di emergenza	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relationa l Database Service (Amazon RDS). Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender e le operazioni del database non appena il failover è completat o.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.E	CP-2.E Piano di emergenza	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.E	CP-2.E Piano di emergenza	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CCCS-fPBMM-CP-2.E	CP-2.E Piano di emergenza	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.F	CP-2.F Piano di emergenza	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.F	CP-2.F Piano di emergenza	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.F	CP-2.F Piano di emergenza	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.F	CP-2.F Piano di emergenza	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.F	CP-2.F Piano di emergenza	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relationa l Database Service (Amazon RDS). Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender e le operazioni del database non appena il failover è completat o.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.F	CP-2.F Piano di emergenza	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.F	CP-2.F Piano di emergenza	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CCCS-fPBMM-CP-2.F	CP-2.F Piano di emergenza	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.G	CP-2.G Piano di emergenza	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.G	CP-2.G Piano di emergenza	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.G	CP-2.G Piano di emergenza	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.G	CP-2.G Piano di emergenza	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.G	CP-2.G Piano di emergenza	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relationa l Database Service (Amazon RDS). Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender e le operazioni del database non appena il failover è completat o.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.G	CP-2.G Piano di emergenza	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-2.G	CP-2.G Piano di emergenza	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CCCS-fPBMM-CP-2.G	CP-2.G Piano di emergenza	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(1)	CP-6(1) Sito di storage alternativo | Separazione dal sito primario	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6(2)	CP-6(2) Sito di storage alternativo | Obiettivi di tempo di ripristino e punto di ripristino	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.A	CP-6.A Sito di storage alternativo	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-6.B	CP-6.B Sito di storage alternativo	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurat i che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionD ays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(3)	CP-9(3) Backup del sistema informativo | Storage separato per informazioni critiche	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(7)	CP-9(7) Backup del sistema informativo | Doppia autorizzazione	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9(7)	CP-9(7) Backup del sistema informativo | Doppia autorizzazione	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.A	CP-9.A Backup del sistema informativo	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.AA	CP-9.AA Backup del sistema informativo	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.B	CP-9.B Backup del sistema informativo	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.C	CP-9.C Backup del sistema informativo	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-9.D	CP-9.D Backup del sistema informativo	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-10.A	CP-10.A Ripristino e ricostituzione del sistema informativo	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-10.A	CP-10.A Ripristino e ricostituzione del sistema informativo	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-10.A	CP-10.A Ripristino e ricostituzione del sistema informativo	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
CCCS-fPBMM-CP-10.A	CP-10.A Ripristino e ricostituzione del sistema informativo	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-10.A	CP-10.A Ripristino e ricostituzione del sistema informativo	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-10.A	CP-10.A Ripristino e ricostituzione del sistema informativo	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-10.A	CP-10.A Ripristino e ricostituzione del sistema informativo	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relationa l Database Service (Amazon RDS). Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender e le operazioni del database non appena il failover è completat o.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-10.A	CP-10.A Ripristino e ricostituzione del sistema informativo	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CCCS-fPBMM-CP-10.A	CP-10.A Ripristino e ricostituzione del sistema informativo	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-10.A	CP-10.A Ripristino e ricostituzione del sistema informativo	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-10.A	CP-10.A Ripristino e ricostituzione del sistema informativo	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-CP-10.A	CP-10.A Ripristino e ricostituzione del sistema informativo	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2(1)	IA-2(1) Identific azione e autentica zione (utenti dell'orga nizzazione) | Accesso alla rete per account con privilegi	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2(1)	IA-2(1) Identificazione e autenticazione (utenti dell'organizzazione) | Accesso alla rete per account con privilegi	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2(1)	IA-2(1) Identificazione e autenticazione (utenti dell'organizzazione) | Accesso alla rete per account con privilegi	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2(3)	IA-2(3) Identificazione e autenticazione (utenti dell'organizzazione) | Accesso locale per account con privilegi	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2(3)	IA-2(3) Identificazione e autenticazione (utenti dell'organizzazione) | Accesso locale per account con privilegi	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2(3)	IA-2(3) Identificazione e autenticazione (utenti dell'organizzazione) | Accesso locale per account con privilegi	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2(8)	IA-2(8) Identificazione e autenticazione (utenti dell'organizzazione) | Accesso alla rete per account con privilegi: resistenza a replay	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2(8)	IA-2(8) Identificazione e autenticazione (utenti dell'organizzazione) | Accesso alla rete per account con privilegi: resistenza a replay	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2(8)	IA-2(8) Identificazione e autenticazione (utenti dell'organizzazione) | Accesso alla rete per account con privilegi: resistenza a replay	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2(11)	IA-2(11) Identificazione e autenticazione (utenti dell'organizzazione) | Accesso agli account: dispositivo separato	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2(11)	IA-2(11) Identificazione e autenticazione (utenti dell'organizzazione) | Accesso agli account: dispositivo separato	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione e alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2(11)	IA-2(11) Identificazione e autenticazione (utenti dell'organizzazione) | Accesso agli account: dispositivo separato	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2.A	IA-2.A Identificazione e autenticazione (utenti dell'orga nizzazione)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2.A	IA-2.A Identificazione e autenticazione (utenti dell'orga nizzazione)	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2.A	IA-2.A Identificazione e autenticazione (utenti dell'orga nizzazione)	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-2.A	IA-2.A Identificazione e autenticazione (utenti dell'organizzazione)	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4(4)	IA-4(4) Gestione degli identificatori | Identificazione dello stato dell'utente	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.A	IA-4.A Gestione degli identificatori	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.A	IA-4.A Gestione degli identificatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.A	IA-4.A Gestione degli identificatori	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.B	IA-4.B Gestione degli identificatori	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.B	IA-4.B Gestione degli identificatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.B	IA-4.B Gestione degli identificatori	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.C	IA-4.C Gestione degli identificatori	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.C	IA-4.C Gestione degli identificatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.C	IA-4.C Gestione degli identificatori	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.D	IA-4.D Gestione degli identificatori	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.D	IA-4.D Gestione degli identificatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.D	IA-4.D Gestione degli identificatori	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.E	IA-4.E Gestione degli identificatori	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.E	IA-4.E Gestione degli identificatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-4.E	IA-4.E Gestione degli identificatori	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5(1)	IA-5(1) Gestione degli autenticatori | Autenticazione basata su password	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5(2)	IA-5(2) Gestione degli autenticatori | Autenticazione basata su PKI	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
CCCS-fPBMM-IA-5(2)	IA-5(2) Gestione degli autenticatori | Autenticazione basata su PKI	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5(4)	IA-5(4) Gestione degli autenticatori | Supporto automatizzato per la determinazione della complessità delle password	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5(8)	IA-5(8) Gestione degli autenticatori | Account multipli del sistema informativo	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5(8)	IA-5(8) Gestione degli autenticatori | Account multipli del sistema informativo	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5(8)	IA-5(8) Gestione degli autenticatori | Account multipli del sistema informativo	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.A	IA-5.A Gestione degli autenticatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.A	IA-5.A Gestione degli autenticatori	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.A	IA-5.A Gestione degli autenticatori	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.A	IA-5.A Gestione degli autenticatori	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.B	IA-5.B Gestione degli autenticatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.B	IA-5.B Gestione degli autenticatori	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.B	IA-5.B Gestione degli autenticatori	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.B	IA-5.B Gestione degli autenticatori	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.C	IA-5.C Gestione degli autenticatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.C	IA-5.C Gestione degli autenticatori	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.C	IA-5.C Gestione degli autenticatori	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.C	IA-5.C Gestione degli autenticatori	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.D	IA-5.D Gestione degli autenticatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.D	IA-5.D Gestione degli autenticatori	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.D	IA-5.D Gestione degli autenticatori	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.D	IA-5.D Gestione degli autenticatori	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.E	IA-5.E Gestione degli autenticatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.E	IA-5.E Gestione degli autenticatori	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.E	IA-5.E Gestione degli autenticatori	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.E	IA-5.E Gestione degli autenticatori	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.F	IA-5.F Gestione degli autenticatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.F	IA-5.F Gestione degli autenticatori	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.F	IA-5.F Gestione degli autenticatori	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.F	IA-5.F Gestione degli autenticatori	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.G	IA-5.G Gestione degli autenticatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.G	IA-5.G Gestione degli autenticatori	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.G	IA-5.G Gestione degli autenticatori	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.G	IA-5.G Gestione degli autenticatori	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.H	IA-5.H Gestione degli autenticatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.H	IA-5.H Gestione degli autenticatori	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.H	IA-5.H Gestione degli autenticatori	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.H	IA-5.H Gestione degli autenticatori	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.I	IA-5.I Gestione degli autenticatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.I	IA-5.I Gestione degli autenticatori	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.I	IA-5.I Gestione degli autenticatori	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.I	IA-5.I Gestione degli autenticatori	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.J	IA-5.J Gestione degli autenticatori	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.J	IA-5.J Gestione degli autenticatori	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.J	IA-5.J Gestione degli autenticatori	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IA-5.J	IA-5.J Gestione degli autenticatori	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-IR-6(1)	IR-6(1) Segnalazione degli incidenti | Segnalazione automatica	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MA-3.A	MA-3.A Strumenti di manutenzione	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MA-3.A	MA-3.A Strumenti di manutenzione	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CCCS-fPBMM-MA-4(1)	MA-4(1) Manutenzione non locale | Audit e revisione	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MA-4(1)	MA-4(1) Manutenzione non locale | Audit e revisione	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
CCCS-fPBMM-MA-4(1)	MA-4(1) Manutenzione non locale | Audit e revisione	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MA-4(1)	MA-4(1) Manutenzione non locale | Audit e revisione	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MA-4(1)	MA-4(1) Manutenzione non locale | Audit e revisione	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MA-4(1)	MA-4(1) Manutenzione non locale | Audit e revisione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MA-4(1)	MA-4(1) Manutenzione non locale | Audit e revisione	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MA-4(1)	MA-4(1) Manutenzione non locale | Audit e revisione	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MA-4(1)	MA-4(1) Manutenzione non locale | Audit e revisione	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MA-4(1)	MA-4(1) Manutenzione non locale | Audit e revisione	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MA-4(1)	MA-4(1) Manutenzione non locale | Audit e revisione	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-MP-2.A	MP-2.A Accesso multimediale	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-RA-5.A	RA-5.A Scansione delle vulnerabilità	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-RA-5.B	RA-5.B Scansione delle vulnerabilità	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-RA-5.C	RA-5.C Scansione delle vulnerabilità	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-RA-5.D	RA-5.D Scansione delle vulnerabilità	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-RA-5.E	RA-5.E Scansione delle vulnerabilità	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SA-10(1)	SA-10(1) Gestione della configurazione per sviluppatori | Verifica dell'integrità di software e firmware	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-5.A	SC-5.A Protezione Denial of Service	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-5.A	SC-5.A Protezione Denial of Service	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilità delle risorse	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilità delle risorse	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilità delle risorse	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilità delle risorse	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilità delle risorse	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilità delle risorse	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relationa l Database Service (Amazon RDS). Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender e le operazioni del database non appena il failover è completat o.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilità delle risorse	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CCCS-fPBMM-SC-6.A	SC-6.A Disponibilità delle risorse	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(3)	SC-7(3) Protezione dei confini | Punti di accesso	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(4)	SC-7(4) Protezione dei confini | Servizi di telecomunicazione esterni	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(5)	SC-7(5) Protezione dei confini | Rifiuto per impostazi one predefinita e consenso in via eccezionale	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(5)	SC-7(5) Protezione dei confini | Rifiuto per impostazione predefinita e consenso in via eccezionale	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(5)	SC-7(5) Protezione dei confini | Rifiuto per impostazi one predefinita e consenso in via eccezionale	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(5)	SC-7(5) Protezione dei confini | Rifiuto per impostazi one predefinita e consenso in via eccezionale	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7(7)	SC-7(7) Protezione dei confini | Prevenzione del tunneling split per dispositivi remoti	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.A	SC-7.A Protezione dei confini	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.B	SC-7.B Protezione dei confini	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-7.C	SC-7.C Protezione dei confini	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-8(1)	SC-8(1) Riservatezza e integrità della trasmissione | Protezione fisica crittografica o alternativa	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-SC-8(1)	SC-8(1) Riservatezza e integrità della trasmissione | Protezione fisica crittografica o alternativa	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-8(1)	SC-8(1) Riservatezza e integrità della trasmissione | Protezione fisica crittografica o alternativa	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-8(1)	SC-8(1) Riservatezza e integrità della trasmissione | Protezione fisica crittografica o alternativa	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-8(1)	SC-8(1) Riservatezza e integrità della trasmissione | Protezione fisica crittografica o alternativa	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
CCCS-fPBMM-SC-8(1)	SC-8(1) Riservatezza e integrità della trasmissione | Protezione fisica crittografica o alternativa	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-8(1)	SC-8(1) Riservatezza e integrità della trasmissione | Protezione fisica crittografica o alternativa	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-SC-8(1)	SC-8(1) Riservatezza e integrità della trasmissione | Protezione fisica crittografica o alternativa	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-8(1)	SC-8(1) Riservatezza e integrità della trasmissione | Protezione fisica crittografica o alternativa	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-SC-8.A	SC-8.A Riservatezza e integrità della trasmissione	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-8.A	SC-8.A Riservatezza e integrità della trasmissione	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
CCCS-fPBMM-SC-8.A	SC-8.A Riservatezza e integrità della trasmissione	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-8.A	SC-8.A Riservatezza e integrità della trasmissione	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-8.A	SC-8.A Riservatezza e integrità della trasmissione	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
CCCS-fPBMM-SC-8.A	SC-8.A Riservatezza e integrità della trasmissione	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-8.A	SC-8.A Riservatezza e integrità della trasmissione	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-SC-8.A	SC-8.A Riservatezza e integrità della trasmissione	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-8.A	SC-8.A Riservatezza e integrità della trasmissione	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-12(1)	SC-12(1) Creazione e gestione delle chiavi crittografiche | Disponibilità	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che le chiavi master del cliente (CMK) necessarie non siano pianificate per l'eliminazione in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
CCCS-fPBMM-SC-12(2)	SC-12(2) Creazione e gestione delle chiavi crittografiche | Chiavi simmetriche	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-12(2)	SC-12(2) Creazione e gestione delle chiavi crittografiche | Chiavi simmetriche	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel servizio di gestione delle AWS chiavi (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
CCCS-fPBMM-SC-12.A	SC-12.A Creazione e gestione delle chiavi crittografiche	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-12.A	SC-12.A Creazione e gestione delle chiavi crittografiche	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel servizio di gestione delle AWS chiavi (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-13.A	SC-13.A Protezione crittografica	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-22.A	SC-22.A Architettura e provisioning per il servizio di risoluzione di nomi e indirizzi	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
CCCS-fPBMM-SC-23.A	SC-23.A Autenticità della sessione	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-23.A	SC-23.A Autenticità della sessione	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
CCCS-fPBMM-SC-23.A	SC-23.A Autenticità della sessione	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-23.A	SC-23.A Autenticità della sessione	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-23.A	SC-23.A Autenticità della sessione	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
CCCS-fPBMM-SC-23.A	SC-23.A Autenticità della sessione	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-23.A	SC-23.A Autenticità della sessione	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-SC-23.A	SC-23.A Autenticità della sessione	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-23.A	SC-23.A Autenticità della sessione	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28(1)	SC-28(1) Protezione delle informazioni a riposo | Protezione crittografica	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SC-28.A	SC-28.A Protezione delle informazioni a riposo	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2(2)	SI-2(2) Correzione dei difetti | Stato della correzione automatizzata dei difetti	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2(2)	SI-2(2) Correzione dei difetti | Stato della correzione automatizzata dei difetti	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2(2)	SI-2(2) Correzione dei difetti | Stato della correzione automatizzata dei difetti	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2(2)	SI-2(2) Correzione dei difetti | Stato della correzione automatizzata dei difetti	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-SI-2(2)	SI-2(2) Correzione dei difetti | Stato della correzione automatizzata dei difetti	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2(2)	SI-2(2) Correzione dei difetti | Stato della correzione automatizzata dei difetti	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2(2)	SI-2(2) Correzione dei difetti | Stato della correzione automatizzata dei difetti	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2(2)	SI-2(2) Correzione dei difetti | Stato della correzione automatizzata dei difetti	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2(2)	SI-2(2) Correzione dei difetti | Stato della correzione automatizzata dei difetti	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
CCCS-fPBMM-SI-2(2)	SI-2(2) Correzione dei difetti | Stato della correzione automatizzata dei difetti	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2(2)	SI-2(2) Correzione dei difetti | Stato della correzione automatizzata dei difetti	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2(2)	SI-2(2) Correzione dei difetti | Stato della correzione automatizzata dei difetti	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2(3)	SI-2(3) Correzione dei difetti | Tempo di correzione dei difetti / Benchmark per le azioni correttive	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.A	SI-2.A Correzione dei difetti	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.A	SI-2.A Correzione dei difetti	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.A	SI-2.A Correzione dei difetti	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.A	SI-2.A Correzione dei difetti	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-SI-2.A	SI-2.A Correzione dei difetti	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.A	SI-2.A Correzione dei difetti	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.A	SI-2.A Correzione dei difetti	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.A	SI-2.A Correzione dei difetti	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.A	SI-2.A Correzione dei difetti	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
CCCS-fPBMM-SI-2.A	SI-2.A Correzione dei difetti	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.A	SI-2.A Correzione dei difetti	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.A	SI-2.A Correzione dei difetti	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.B	SI-2.B Correzione dei difetti	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.B	SI-2.B Correzione dei difetti	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.B	SI-2.B Correzione dei difetti	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.B	SI-2.B Correzione dei difetti	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-SI-2.B	SI-2.B Correzione dei difetti	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.B	SI-2.B Correzione dei difetti	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.B	SI-2.B Correzione dei difetti	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.B	SI-2.B Correzione dei difetti	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.B	SI-2.B Correzione dei difetti	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
CCCS-fPBMM-SI-2.B	SI-2.B Correzione dei difetti	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.B	SI-2.B Correzione dei difetti	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.B	SI-2.B Correzione dei difetti	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.C	SI-2.C Correzione dei difetti	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.C	SI-2.C Correzione dei difetti	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.C	SI-2.C Correzione dei difetti	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.C	SI-2.C Correzione dei difetti	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-SI-2.C	SI-2.C Correzione dei difetti	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.C	SI-2.C Correzione dei difetti	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.C	SI-2.C Correzione dei difetti	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.C	SI-2.C Correzione dei difetti	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.C	SI-2.C Correzione dei difetti	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
CCCS-fPBMM-SI-2.C	SI-2.C Correzione dei difetti	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.C	SI-2.C Correzione dei difetti	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.C	SI-2.C Correzione dei difetti	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.D	SI-2.D Correzione dei difetti	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.D	SI-2.D Correzione dei difetti	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.D	SI-2.D Correzione dei difetti	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.D	SI-2.D Correzione dei difetti	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CCCS-fPBMM-SI-2.D	SI-2.D Correzione dei difetti	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.D	SI-2.D Correzione dei difetti	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.D	SI-2.D Correzione dei difetti	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.D	SI-2.D Correzione dei difetti	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.D	SI-2.D Correzione dei difetti	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
CCCS-fPBMM-SI-2.D	SI-2.D Correzione dei difetti	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.D	SI-2.D Correzione dei difetti	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-2.D	SI-2.D Correzione dei difetti	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3(1)	SI-3(1) Protezione da codice dannoso | Gestione centrale	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3(7)	SI-3(7) Protezione da codice dannoso | Rilevamento non basato sulla firma	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.A	SI-3.A Protezione da codice dannoso	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.A	SI-3.A Protezione da codice dannoso	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.A	SI-3.A Protezione da codice dannoso	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.A	SI-3.A Protezione da codice dannoso	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.A	SI-3.A Protezione da codice dannoso	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.B	SI-3.B Protezione da codice dannoso	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.B	SI-3.B Protezione da codice dannoso	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.B	SI-3.B Protezione da codice dannoso	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.B	SI-3.B Protezione da codice dannoso	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.C	SI-3.C Protezione da codice dannoso	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.C	SI-3.C Protezione da codice dannoso	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.C	SI-3.C Protezione da codice dannoso	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.C	SI-3.C Protezione da codice dannoso	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.D	SI-3.D Protezione da codice dannoso	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.D	SI-3.D Protezione da codice dannoso	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.D	SI-3.D Protezione da codice dannoso	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-3.D	SI-3.D Protezione da codice dannoso	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(1)	SI-4(1) Monitoraggio del sistema informativo | Sistema di rilevamento delle intrusioni a livello di sistema	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(1)	SI-4(1) Monitoraggio del sistema informativo | Sistema di rilevamento delle intrusioni a livello di sistema	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(2)	SI-4(2) Monitoraggio del sistema informativo | Strumenti automatizzati per l'analisi in tempo reale	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(2)	SI-4(2) Monitoraggio del sistema informati vo | Strumenti automatizzati per l'analisi in tempo reale	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(4)	SI-4(4) Monitoraggio del sistema | Traffico di comunicazioni in entrata e in uscita	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(4)	SI-4(4) Monitoraggio del sistema | Traffico di comunicazioni in entrata e in uscita	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(5)	SI-4(5) Monitoraggio del sistema informativo | Avvisi generati dal sistema	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(11)	SI-4(11) Monitoraggio del sistema informativo | Analisi delle anomalie del traffico di comunicazione	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(11)	SI-4(11) Monitoraggio del sistema informativo | Analisi delle anomalie del traffico di comunicazione	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(16)	SI-4(16) Monitoraggio del sistema informativo | Correlazione delle informazioni di monitoraggio	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(16)	SI-4(16) Monitoraggio del sistema informativo | Correlazione delle informazioni di monitoraggio	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(20)	SI-4(20) Monitoraggio del sistema informativo | Utente con privilegi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(23)	SI-4(23) Monitoraggio del sistema informativo | Dispositivi basati su host	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di gestione e le chiamate API. AWS È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4(23)	SI-4(23) Monitoraggio del sistema informativo | Dispositivi basati su host	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.A	SI-4.A Monitoraggio del sistema informativo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.A	SI-4.A Monitoraggio del sistema informativo	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.A	SI-4.A Monitoraggio del sistema informativo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
CCCS-fPBMM-SI-4.A	SI-4.A Monitoraggio del sistema informativo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.A	SI-4.A Monitoraggio del sistema informativo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.B	SI-4.B Monitoraggio del sistema informativo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.B	SI-4.B Monitoraggio del sistema informativo	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.B	SI-4.B Monitoraggio del sistema informativo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
CCCS-fPBMM-SI-4.B	SI-4.B Monitoraggio del sistema informativo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.B	SI-4.B Monitoraggio del sistema informativo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.C	SI-4.C Monitoraggio del sistema informativo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.C	SI-4.C Monitoraggio del sistema informativo	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.C	SI-4.C Monitoraggio del sistema informativo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
CCCS-fPBMM-SI-4.C	SI-4.C Monitoraggio del sistema informativo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.C	SI-4.C Monitoraggio del sistema informativo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.D	SI-4.D Monitoraggio del sistema informativo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.D	SI-4.D Monitoraggio del sistema informativo	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.D	SI-4.D Monitoraggio del sistema informativo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
CCCS-fPBMM-SI-4.D	SI-4.D Monitoraggio del sistema informativo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.D	SI-4.D Monitoraggio del sistema informativo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.E	SI-4.E Monitoraggio del sistema informativo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.E	SI-4.E Monitoraggio del sistema informativo	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.E	SI-4.E Monitoraggio del sistema informativo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
CCCS-fPBMM-SI-4.E	SI-4.E Monitoraggio del sistema informativo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.E	SI-4.E Monitoraggio del sistema informativo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.F	SI-4.F Monitoraggio del sistema informativo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.F	SI-4.F Monitoraggio del sistema informativo	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.F	SI-4.F Monitoraggio del sistema informativo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
CCCS-fPBMM-SI-4.F	SI-4.F Monitoraggio del sistema informativo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.F	SI-4.F Monitoraggio del sistema informativo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.G	SI-4.G Monitoraggio del sistema informativo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.G	SI-4.G Monitoraggio del sistema informativo	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.G	SI-4.G Monitoraggio del sistema informativo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
CCCS-fPBMM-SI-4.G	SI-4.G Monitoraggio del sistema informativo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-4.G	SI-4.G Monitoraggio del sistema informativo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-5.A	SI-5.A Avvisi, consigli e direttive di sicurezza	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-5.B	SI-5.B Avvisi, consigli e direttive di sicurezza	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-5.C	SI-5.C Avvisi, consigli e direttive di sicurezza	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-5.D	SI-5.D Avvisi, consigli e direttive di sicurezza	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-7(1)	SI-7(1) Integrità di software, firmware e informazioni | Controlli di integrità	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-7(7)	SI-7(7) Integrità di software, firmware e informazioni | Integrazione di rilevamento e risposta	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-7.A	SI-7.A Integrità di software, firmware e informazioni	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CCCS-fPBMM-SI-12.A	SI-12.A Gestione e conservazione delle informazioni	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile.

Best practice operative per CIS AWS Foundations Benchmark v1.4 Level 1

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra Amazon Web Services Foundation v1.4 Level 1 del Center for Internet Security (CIS) e le regole di AWS Config/Process Checks gestite.AWS Config Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CIS di

Amazon Web Services Foundation v1.4 Level 1. Un controllo CIS Amazon Web Services Foundation v1.4 Livello 1 può essere associato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Per ulteriori informazioni sui controlli di processo, consulta process-checks.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.1	Mantiene i dettagli di contatto attuali	account-contact-details-configured (controllo del processo)	Verifica che l'indirizzo e-mail e il numero di telefono di contatto degli account AWS siano aggiornati e che corrispondano a più di un individuo della tua organizzazione. Nella sezione Il mio account della console, verifica la correttezza delle informazioni specificate nella sezione Informazioni di contatto. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2	Verifica che le informazioni di contatto di sicurezza siano registrate	account-security-contact-configured (Controllo del processo)	Assicurati che l'indirizzo e-mail e il numero di telefono di contatto del team di sicurezza della tua organizzazione siano aggiornati. Nella sezione Il mio account della Console di AWS gestione, assicurati che le informazioni corrette siano specificate nella sezione Sicurezza. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.4	Verifica non esistano chiavi di accesso dell'utente "root"	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.5	Verifica che l'autenticazione a più fattori sia abilitata per l'utente "root"	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1,7	Elimina l'uso dell'utente "root" per le attività amministrative e quotidiane	root-account-regular-use (Controllo del processo)	Assicurati che per le attività quotidiane non venga utilizzato l'account root. All'interno di IAM, esegui un report sulle credenziali per verificare quando l'utente root è stato utilizzato per l'ultima volta. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.8	Verifica che la policy delle password IAM richieda una lunghezza minima di 14 o più caratteri	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.9	Verifica che la policy delle password di IAM impedisca il riutilizzo delle password	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.10	Verifica se autentica zione a più fattori (MFA) è abilitata per tutti gli utenti che dispongono di una password per la console	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.11	Non configurare le chiavi di accesso durante la configura zione iniziale per tutti gli utenti che dispongono di una password per la console	iam-user-console-and- (Controllo del processo) api-access-at-creation	Assicurati che le chiavi di accesso non vengano configurate durante la configura zione iniziale per tutti gli utenti che dispongono di una password per la console. Per tutti gli utenti con accesso alla console, confronta l'ora di creazione dell'uten te con la data di creazione della chiave di accesso. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundatio ns Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.12	Verifica che le credenziali non utilizzate per 45 giorni o più siano disabilitate	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede l'impostazione di un valore per l' maxCredentialUsageetà (valore standard CIS: 45). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.13	Assicurati che sia disponibile una sola chiave di accesso attiva per ogni utente.	iam- user-single-access-key (Controllo del processo)	Assicurati che sia disponibile una sola chiave di accesso attiva per ogni utente. Per tutti gli utenti, verifica che nella scheda Credenziali di sicurezza venga utilizzata una sola chiave attiva per ogni utente all'interno di IAM. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.14	Verifica che le chiavi di accesso vengano ruotate ogni 90 giorni o meno	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.15	Verifica che gli utenti ricevano le autorizzazioni solo tramite gruppi	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.15	Verifica che gli utenti ricevano le autorizzazioni solo tramite gruppi	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.15	Verifica che gli utenti ricevano le autorizzazioni solo tramite gruppi	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.16	Verifica che non siano associate policy IAM che consentono privilegi amministrativi "*:*" completi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1,17	Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support	iam-policy-in-use	AWS Identity and Access Managemen t (IAM) può aiutarti a gestire i permessi e le autorizzazioni di accesso assicuran do che le policy IAM siano assegnate agli utenti, ai ruoli o ai gruppi appropria ti. La limitazione di queste policy include anche i principi del privilegio minimo e della separazione dei compiti. Questa regola richiede l'impostazione di Policyarn su arn:aws:i am: :aws:policy/, per la gestione degli incidenti con Support. AWSSupportAccess AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.19	Assicurati che tutti i certificati SSL/TLS scaduti archiviati in AWS IAM vengano rimossi	iam-expired-certificates (Controllo del processo)	Assicurati che tutti i certificati SSL/TLS scaduti archiviati in IAM vengano rimossi. Dalla riga di comando con la AWS CLI installata esegui il comando 'AWS iam list-server-certificates' e determina se ci sono certificati server scaduti. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.20	Assicurati che AWS IAM Access Analyzer sia abilitato	iam-access-analyzer-enabled (Controllo del processo)	Assicurati che Sistema di analisi degli accessi IAM sia abilitato. Nella sezione IAM della console, seleziona Analizzatore di accessi e assicurati che STATO sia impostato su Attivo. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1.3	Verifica che la funzionalità MFA Delete sia abilitata sui bucket S3	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. L'aggiunta dell'eliminazione dell'autenticazione a più fattori (MFA) a un bucket S3 richiede un fattore di autenticazione aggiuntivo per modificare lo stato della versione del bucket o eliminare una versione dell'oggetto. La funzionalità MFA Delete può aggiungere un ulteriore livello di sicurezza nel caso in cui le credenziali di sicurezza vengano compromesse o venga concesso un accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1.5	Verifica se i bucket S3 sono configurati con "Blocca accesso pubblico (Impostazioni bucket)"	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1.5	Verifica se i bucket S3 sono configurati con "Blocca accesso pubblico (Impostazioni bucket)"	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
2.2.1	Verifica se la crittografia dei volumi EBS è attiva	encrypted-volumes	Poiché possono esistere dati sensibili, per proteggere i dati a riposo assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.1	Verifica se la crittografia dei volumi EBS è attiva	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
2.3.1	Verifica se la crittografia è abilitata per le istanze RDS	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.3.1	Verifica se la crittografia è abilitata per le istanze RDS	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1	Ensure CloudTrail è abilitato in tutte le regioni	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Assicurati che il bucket S3 utilizzato per archiviare CloudTrail i log non sia accessibile al pubblico	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.3	Assicurati che il bucket S3 utilizzato per archiviare CloudTrail i log non sia accessibile al pubblico	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Assicurati che il bucket S3 utilizzato per archiviare CloudTrail i log non sia accessibile al pubblico	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
3.4	Assicurati che i CloudTrail percorsi siano integrati con Logs CloudWatch	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6	Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle chiamate API non autorizzate	alarm-unauthorized-api-calls (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle chiamate API non autorizzate. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.2	Verifica se esistono un filtro e un allarme per le metriche dei log per l'accesso alla Console di gestione senza autenticazione a più fattori (MFA)	allarme- sign-in-without-mfa (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente all'accesso alla Console di gestione AWS senza l'autenticazione a più fattori (MFA). Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.3	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente all'utilizzo dell'account "root"	alarm-root-account-use (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente all'utilizzo dell'account "root". Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle policy IAM	alarm-iam-policy-change (Controllo del processo)	Verifica che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alla policy IAM. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.5	Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrail alla configurazione	alarm-cloudtrail-config-change (Controllo del processo)	Assicurati che esista un filtro metrico di registro e un allarme per le modifiche AWS CloudTrail alla configurazione. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle policy dei bucket S3	alarm-s3- (controllo del processo) bucket-policy-change	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alla policy del bucket Amazon S3. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundatio ns Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.12	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ai gateway di rete	allarme- vpc-network-gateway-change (controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ai gateway di rete. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.13	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle tabelle di routing	allarme- vpc-route-table-change (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle tabelle di routing Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.14	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate al VPC	alarm-vpc-change (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ad Amazon Virtual Private Cloud (VPC). Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundatio ns Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.15	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ad AWS Organizations	alarm-organizations-change (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ad AWS Organizations Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.1	Verifica se le liste di controllo degli accessi alla rete consentono l'ingresso da 0.0.0.0/0 alle porte di amministrazione del server remoto	nacl-no-unrestricted-ssh-rdp	Assicurati che le liste di controllo degli accessi alla rete consentano l'ingresso pubblico alle porte di amministrazione del server remoto. All'interno della sezione VPC della console, assicurati che siano presenti liste di controllo degli accessi alla rete con origine "0.0.0.0/0" e con porte o intervalli di porte abilitate, comprese le porte di amministrazione del server remoto. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Verifica se i gruppi di sicurezza consentono l'ingresso da 0.0.0.0/0 alle porte di amministrazione del server remoto	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Verifica se i gruppi di sicurezza consentono l'ingresso da 0.0.0.0/0 alle porte di amministrazione del server remoto	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valore standard CIS: 3389). I valori effettivi devono riflettere le policy dell'organizzazione.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 1.

Best practice operative per CIS AWS Foundations Benchmark v1.4 Level 2

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra Amazon Web Services Foundation v1.4 Level 2 del Center for Internet Security (CIS) e le regole di AWS Config/Process Checks gestite.AWS Config Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CIS di Amazon Web Services Foundation v1.4 Level 2. Un controllo CIS Amazon Web Services Foundation v1.4 Livello 2 può essere associato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Per ulteriori informazioni sui controlli di processo, consulta process-checks.

Regione AWS: Tutti i paesi Regioni AWS in cui sono supportati i pacchetti di conformità (supporto regionale) tranne (Stati Uniti orientali), AWS GovCloud (Stati Uniti occidentali) e Medio Oriente AWS GovCloud (Bahrein)

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.1	Mantiene i dettagli di contatto attuali	account-contact-details-configured (controllo del processo)	Verifica che l'indirizzo e-mail e il numero di telefono di contatto degli account AWS siano aggiornati e che corrispondano a più di un individuo della tua organizzazione. Nella sezione Il mio account della console, verifica la correttezza delle informazioni specificate nella

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			sezione Informazioni di contatto. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2	Verifica che le informazioni di contatto di sicurezza siano registrate	account-security-contact-configured (Controllo del processo)	Assicurati che l'indirizzo e-mail e il numero di telefono di contatto del team di sicurezza della tua organizzazione siano aggiornati. Nella sezione Il mio account della Console di AWS gestione, assicurati che le informazioni corrette siano specificate nella sezione Sicurezza. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.4	Verifica non esistano chiavi di accesso dell'utente "root"	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.5	Verifica che l'autenticazione a più fattori sia abilitata per l'utente "root"	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.6	Assicurati che l'autenticazione a più fattori sia abilitata per l'utente "root"	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1,7	Elimina l'uso dell'utente "root" per le attività amministrative e quotidiane	root-account-regular-use (Controllo del processo)	Assicurati che per le attività quotidiane non venga utilizzato l'account root. All'interno di IAM, esegui un report sulle credenziali per verificare quando l'utente root è stato utilizzato per l'ultima volta. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.8	Verifica che la policy delle password IAM richieda una lunghezza minima di 14 o più caratteri	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.9	Verifica che la policy delle password di IAM impedisca il riutilizzo delle password	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.10	Verifica se autentica zione a più fattori (MFA) è abilitata per tutti gli utenti che dispongono di una password per la console	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.11	Non configurare le chiavi di accesso durante la configura zione iniziale per tutti gli utenti che dispongono di una password per la console	iam-user-console-and- (Controllo del processo) api-access-at-creation	Assicurati che le chiavi di accesso non vengano configurate durante la configura zione iniziale per tutti gli utenti che dispongono di una password per la console. Per tutti gli utenti con accesso alla console, confronta l'ora di creazione dell'uten te con la data di creazione della chiave di accesso. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundatio ns Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.12	Verifica che le credenziali non utilizzate per 45 giorni o più siano disabilitate	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede l'impostazione di un valore per l' maxCredentialUsageetà (valore standard CIS: 45). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.13	Assicurati che sia disponibile una sola chiave di accesso attiva per ogni utente.	iam- user-single-access-key (Controllo del processo)	Assicurati che sia disponibile una sola chiave di accesso attiva per ogni utente. Per tutti gli utenti, verifica che nella scheda Credenziali di sicurezza venga utilizzata una sola chiave attiva per ogni utente all'interno di IAM. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.14	Verifica che le chiavi di accesso vengano ruotate ogni 90 giorni o meno	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.15	Verifica che gli utenti ricevano le autorizzazioni solo tramite gruppi	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.15	Verifica che gli utenti ricevano le autorizza zioni solo tramite gruppi	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.15	Verifica che gli utenti ricevano le autorizzazioni solo tramite gruppi	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.16	Verifica che non siano associate policy IAM che consentono privilegi amministrativi "*:*" completi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1,17	Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support	iam-policy-in-use	AWS Identity and Access Managemen t (IAM) può aiutarti a gestire i permessi e le autorizzazioni di accesso assicuran do che le policy IAM siano assegnate agli utenti, ai ruoli o ai gruppi appropria ti. La limitazione di queste policy include anche i principi del privilegio minimo e della separazione dei compiti. Questa regola richiede l'impostazione di Policyarn su arn:aws:i am: :aws:policy/, per la gestione degli incidenti con Support. AWSSupportAccess AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.18	Assicurati che i ruoli delle istanze IAM vengano utilizzati per l'accesso alle AWS risorse dalle istanze	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.19	Assicurati che tutti i certificati SSL/TLS scaduti archiviati in AWS IAM vengano rimossi	iam-expired-certificates (Controllo del processo)	Assicurati che tutti i certificati SSL/TLS scaduti archiviati in IAM vengano rimossi. Dalla riga di comando con la AWS CLI installata esegui il comando 'AWS iam list-server-certificates' e determina se ci sono certificati server scaduti. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.20	Assicurati che AWS IAM Access Analyzer sia abilitato	iam-access-analyzer-enabled (Controllo del processo)	Assicurati che Sistema di analisi degli accessi IAM sia abilitato. Nella sezione IAM della console, seleziona Analizzatore di accessi e assicurati che STATO sia impostato su Attivo. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.21	Garantisci la gestione centralizzata degli utenti tramite la federazione delle identità o AWS Organizations per ambienti multi-account	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
2.1.1	Assicurati che tutti i bucket S3 utilizzino encryption-at-rest	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1.2	Verifica se la policy dei bucket S3 è impostata in modo da rifiutare le richieste HTTP	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1.3	Verifica che la funzionalità MFA Delete sia abilitata sui bucket S3	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. L'aggiunta dell'eliminazione dell'autenticazione a più fattori (MFA) a un bucket S3 richiede un fattore di autenticazione aggiuntivo per modificare lo stato della versione del bucket o eliminare una versione dell'oggetto. La funzionalità MFA Delete può aggiungere un ulteriore livello di sicurezza nel caso in cui le credenziali di sicurezza vengano compromesse o venga concesso un accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1.5	Verifica se i bucket S3 sono configurati con "Blocca accesso pubblico (Impostazioni bucket)"	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1.5	Verifica se i bucket S3 sono configurati con "Blocca accesso pubblico (Impostazioni bucket)"	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
2.2.1	Verifica se la crittografia dei volumi EBS è attiva	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.1	Verifica se la crittografia dei volumi EBS è attiva	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
2.3.1	Verifica se la crittografia è abilitata per le istanze RDS	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.3.1	Verifica se la crittografia è abilitata per le istanze RDS	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1	Ensure CloudTrail è abilitato in tutte le regioni	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2	Assicurati che la convalida dei file di CloudTrail registro sia abilitata	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Assicurati che il bucket S3 utilizzato per archiviare CloudTrail i log non sia accessibile al pubblico	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.3	Assicurati che il bucket S3 utilizzato per archiviare CloudTrail i log non sia accessibile al pubblico	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Assicurati che il bucket S3 utilizzato per archiviare CloudTrail i log non sia accessibile al pubblico	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
3.4	Assicurati che i CloudTrail percorsi siano integrati con Logs CloudWatch	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5	Assicurati che AWS Config sia abilitato in tutte le regioni	config-enabled-all-regions (Controllo del processo)	Assicurati che AWS Config sia abilitato in tutte le AWS regioni. Nella sezione AWS Config della console, per ogni regione abilitata assicurati che il registratore AWS Config sia configura to correttamente. Assicurati che la registrazione delle risorse AWS globali sia abilitata almeno in una regione. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundatio ns Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6	Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.7	Assicurati che i CloudTrail log siano crittografati quando sono inattivi utilizzan do le CMK KMS	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail
3.8	Verifica se la rotazione delle chiavi CMK create dal cliente è abilitata	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.
3.9	Verifica se il log del flusso VPC è abilitata in tutti i VPC	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.10	Verifica se i log a livello di oggetto per gli eventi di scrittura sono abilitati per il bucket S3	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
3,11	Verifica se i log a livello di oggetto per gli eventi di lettura sono abilitati per il bucket S3	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle chiamate API non autorizzate	alarm-unauthorized-api-calls (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle chiamate API non autorizzate. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.2	Verifica se esistono un filtro e un allarme per le metriche dei log per l'accesso alla Console di gestione senza autenticazione a più fattori (MFA)	allarme- sign-in-without-mfa (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente all'accesso alla Console di gestione AWS senza l'autenticazione a più fattori (MFA). Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.3	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente all'utilizzo dell'account "root"	alarm-root-account-use (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente all'utilizzo dell'account "root". Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle policy IAM	alarm-iam-policy-change (Controllo del processo)	Verifica che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alla policy IAM. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.5	Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche CloudTrail alla configurazione	alarm-cloudtrail-config-change (Controllo del processo)	Assicurati che esista un filtro metrico di registro e un allarme per le modifiche AWS CloudTrail alla configurazione. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.6	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente agli errori di autentica zione della Console di gestione AWS	alarm-console-auth-failures (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente agli errori di autentica zione della Console di gestione AWS . Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundatio ns Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.7	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alla disabilitazione o all'eliminazione pianificata delle chiavi gestite dal cliente (CMK) create dal cliente	alarm-kms- (controllo del processo) disable-or-delete-cmk	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alla disabilitazione o all'eliminazione pianificata delle chiavi gestite dal cliente (CMK) create dal cliente Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundatio ns Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle policy dei bucket S3	alarm-s3- (controllo del processo) bucket-policy-change	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alla policy del bucket Amazon S3. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundatio ns Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.9	Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alla configurazione di AWS Config	alarm-aws-config-change (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alla configurazione di AWS Config. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.10	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate al gruppo di sicurezza	alarm- vpc-security-group-change (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ai gruppi di sicurezza . Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.11	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle liste di controllo degli accessi alla rete (NACL)	alarm-vpc-nacl-change (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle liste di controllo degli accessi alla rete (NACL). Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.12	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ai gateway di rete	allarme- vpc-network-gateway-change (controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ai gateway di rete. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.13	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle tabelle di routing	allarme- vpc-route-table-change (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle tabelle di routing Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.14	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate al VPC	alarm-vpc-change (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ad Amazon Virtual Private Cloud (VPC). Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundatio ns Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.15	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ad AWS Organ izations	alarm-organizations-change (Controllo del processo)	Assicurati che esistano un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ad AWS Organizations Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundatio ns Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.1	Verifica se le liste di controllo degli accessi alla rete consentono l'ingresso da 0.0.0.0/0 alle porte di amministrazione del server remoto	nacl-no-unrestricted-ssh-rdp	Assicurati che le liste di controllo degli accessi alla rete consentano l'ingresso pubblico alle porte di amministrazione del server remoto. All'interno della sezione VPC della console, assicurati che siano presenti liste di controllo degli accessi alla rete con origine "0.0.0.0/0" e con porte o intervalli di porte abilitate, comprese le porte di amministrazione del server remoto. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Verifica se i gruppi di sicurezza consentono l'ingresso da 0.0.0.0/0 alle porte di amministrazione del server remoto	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Verifica se i gruppi di sicurezza consentono l'ingresso da 0.0.0.0/0 alle porte di amministrazione del server remoto	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valore standard CIS: 3389). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.3	Verifica se il gruppo di sicurezza predefini to di ogni VPC limita tutto il traffico	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4	Verifica se le tabelle di routing per la connessione peering VPC dispongono dell'accesso minimo	vpc-peering-least-access (Controllo del processo)	Assicurati che le tabelle di routing per la connessione peering VPC dispongano dell'accesso minimo. All'interno della sezione VPC della console, esamina le voci della tabella di routing per assicurarti che sia instradabile il minor numero di sottoreti o host ai fini della connessione peering. Per ulteriori dettagli sulla procedura di audit di questo controllo, consulta il documento CIS Amazon Web Services Foundations Benchmark versione 1.4.0, disponibile all'indirizzo https://www.cisecurity.org/benchmark/amazon_web_services/

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 2.

Best practice operative per CIS Critical Security Controls v8 IG1

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra Center for Internet Security (CIS) Critical Security Controls v8 IG1 e le regole Config gestite AWS . Ciascuna AWS Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CIS Critical Security Controls v8 IG1. Un controllo CIS Critical Security Controls v8 IG1 può essere correlato a più regole di AWS Config . Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			non utilizzati nel tuo ambiente.
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	vpc-network-acl-un used-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventari o e una gestione accurati del proprio ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	ec2-security-group-attached-to-eni	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambi ente.
2.2	Verifica che il software autorizza to sia attualmente supportato	elastic-beanstalk-managed-updates-en abled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Verifica che il software autorizzato sia attualmente supportato	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Verifica che il software autorizzato sia attualmente supportato	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribuiti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
3.3	Configurazione delle liste di controllo degli accessi	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.3	Configurazione delle liste di controllo degli accessi	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
3.3	Configurazione delle liste di controllo degli accessi	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.3	Configurazione delle liste di controllo degli accessi	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
3.3	Configurazione delle liste di controllo degli accessi	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.3	Configurazione delle liste di controllo degli accessi	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
3.3	Configurazione delle liste di controllo degli accessi	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.3	Configurazione delle liste di controllo degli accessi	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
3.3	Configurazione delle liste di controllo degli accessi	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
3.3	Configurazione delle liste di controllo degli accessi	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegi o minimo, assicurat i che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).
3.3	Configurazione delle liste di controllo degli accessi	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	efs-access-point-enforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.
3.4	Applicazione della conservazione dei dati	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Applicazione della conservazione dei dati	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.
4.1	Definizione e mantenimento di un processo di configurazione sicuro	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	ec2-volume-inuse-c heck	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	redshift-cluster-m aintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizza zione. In particola re, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il. allowVersionUpgrad e Il valore predefini to è true. Inoltre, consente di impostare facoltativamente il preferredMaintenan ceWindow (l'impost azione predefinita è sab: 16:00 -sab: 16:30) e il automated SnapshotRetention periodo (l'impost azione predefinita è 1). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configurazione sicuro	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associati ons per semplific are l'inventario delle piattaforme e delle applicazioni software all'interno di un'organi zzazione. AWS Syste ms Manager assegna uno stato di configura zione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configura zioni delle applicazi oni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	efs-access-point-e nforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.
4.1	Definizione e mantenimento di un processo di configura zione sicuro	secretsmanager-rot ation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianifica zione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromis sione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizza tiva. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.6	Gestione sicura delle risorse e del software aziendali	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
4.6	Gestione sicura delle risorse e del software aziendali	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.6	Gestione sicura delle risorse e del software aziendali	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
4.6	Gestione sicura delle risorse e del software aziendali	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.6	Gestione sicura delle risorse e del software aziendali	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
4.6	Gestione sicura delle risorse e del software aziendali	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.7	Gestione degli account predefiniti su risorse e software aziendali	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.1	Definizione e mantenimento di un inventario degli account	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Utilizzo di password univoche	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Utilizzo di password univoche	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Utilizzo di password univoche	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Utilizzo di password univoche	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.3	Disattivazione degli account dormienti	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4	Limitazione dei privilegi di amministratore agli account amministratore dedicati	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4	Limitazione dei privilegi di amministratore agli account amministratore dedicati	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.4	Richiesta di MFA per l'accesso remoto alla rete	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.4	Richiesta di MFA per l'accesso remoto alla rete	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.4	Richiesta di MFA per l'accesso remoto alla rete	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6,5	Richiesta dell'MFA per l'accesso amministrativo	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1	Definizione e mantenimento di un processo di gestione delle vulnerabilità	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1	Definizione e mantenimento di un processo di gestione delle vulnerabilità	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1	Definizione e mantenimento di un processo di gestione delle vulnerabilità	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
7.3	Esecuzione della gestione automatizzata delle patch del sistema operativo	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.3	Esecuzione della gestione automatizzata delle patch del sistema operativo	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.3	Esecuzione della gestione automatizzata delle patch del sistema operativo	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.4	Esecuzione della gestione automatizzata delle patch delle applicazioni	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.4	Esecuzione della gestione automatizzata delle patch delle applicazioni	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.4	Esecuzione della gestione automatizzata delle patch delle applicazioni	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	Definizione e mantenimento di un processo di gestione dei log di audit	audit-log-policy-exists (Controllo del processo)	Definizione e mantenimento di una policy di gestione dei log di audit che definisca i requisiti di gestione dei log dell'organizzazione. Ciò include, a titolo esemplificativo, la revisione e la conservazione dei log di audit.
8.2	Raccolta dei log di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indiriz zo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
8.2	Raccolta dei log di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.
8.3	Garanzia di un'adeguata archiviazione dei log di controllo	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementazione e gestione di software antimalware	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2	Configurazione degli aggiornamenti automatici delle firme antimalware	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
11.2	Esecuzione di backup automatici	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
11.2	Esecuzione di backup automatici	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.3	Protezione dei dati di ripristino	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
11.3	Protezione dei dati di ripristino	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
11.3	Protezione dei dati di ripristino	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.3	Protezione dei dati di ripristino	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CIS Critical Security Controls v8 IG1.

Best practice operative per CIS Critical Security Controls v8 IG2

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra Center for Internet Security (CIS) Critical Security Controls v8 IG2 e le regole Config gestite AWS . Ciascuna AWS Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CIS Critical Security Controls v8 IG2. Un controllo CIS Critical Security Controls v8 IG2 può essere correlato a più regole di AWS Config . Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			non utilizzati nel tuo ambiente.
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	vpc-network-acl-un used-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventari o e una gestione accurati del proprio ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	ec2-security-group-attached-to-eni	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambi ente.
2.2	Verifica che il software autorizza to sia attualmente supportato	elastic-beanstalk-managed-updates-en abled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Verifica che il software autorizzato sia attualmente supportato	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Verifica che il software autorizzato sia attualmente supportato	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribuiti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.4	Utilizzo di strumenti automatizzati per l'inventario del software	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.4	Utilizzo di strumenti automatizzati per l'inventario del software	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
3.3	Configurazione delle liste di controllo degli accessi	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.3	Configurazione delle liste di controllo degli accessi	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
3.3	Configurazione delle liste di controllo degli accessi	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.3	Configurazione delle liste di controllo degli accessi	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
3.3	Configurazione delle liste di controllo degli accessi	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.3	Configurazione delle liste di controllo degli accessi	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
3.3	Configurazione delle liste di controllo degli accessi	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.3	Configurazione delle liste di controllo degli accessi	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
3.3	Configurazione delle liste di controllo degli accessi	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
3.3	Configurazione delle liste di controllo degli accessi	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).
3.3	Configurazione delle liste di controllo degli accessi	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	efs-access-point-enforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.
3.4	Applicazione della conservazione dei dati	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Applicazione della conservazione dei dati	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.
3,10	Crittografia dei dati sensibili in transito	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,10	Crittografia dei dati sensibili in transito	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
3,10	Crittografia dei dati sensibili in transito	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.10	Crittografia dei dati sensibili in transito	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
3,10	Crittografia dei dati sensibili in transito	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,10	Crittografia dei dati sensibili in transito	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3,10	Crittografia dei dati sensibili in transito	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.10	Crittografia dei dati sensibili in transito	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
3.10	Crittografia dei dati sensibili in transito	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.10	Crittografia dei dati sensibili in transito	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.11	Crittografia dei dati sensibili a riposo	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.11	Crittografia dei dati sensibili a riposo	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
3,11	Crittografia dei dati sensibili a riposo	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
3,11	Crittografia dei dati sensibili a riposo	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,11	Crittografia dei dati sensibili a riposo	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
3.11	Crittografia dei dati sensibili a riposo	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.11	Crittografia dei dati sensibili a riposo	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
3.11	Crittografia dei dati sensibili a riposo	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,11	Crittografia dei dati sensibili a riposo	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
3,11	Crittografia dei dati sensibili a riposo	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,11	Crittografia dei dati sensibili a riposo	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.11	Crittografia dei dati sensibili a riposo	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
3.11	Crittografia dei dati sensibili a riposo	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.11	Crittografia dei dati sensibili a riposo	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.
3.11	Crittografia dei dati sensibili a riposo	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,11	Crittografia dei dati sensibili a riposo	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.11	Crittografia dei dati sensibili a riposo	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
3.11	Crittografia dei dati sensibili a riposo	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	account-part-of-or ganizations	La gestione centraliz zata Account AWS all'interno di AWS Organizations aiuta a garantire la conformit à degli account. L'assenza di una governance centraliz zata degli account può comportar e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
4.1	Definizione e mantenimento di un processo di configura zione sicuro	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	ec2-volume-inuse-c heck	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	redshift-cluster-m aintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizza zione. In particola re, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il. allowVersionUpgrad e Il valore predefini to è true. Inoltre, consente di impostare facoltativamente il preferredMaintenan ceWindow (l'impost azione predefinita è sab: 16:00 -sab: 16:30) e il automated SnapshotRetention periodo (l'impost azione predefinita è 1). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	ec2-instance-manag ed-by-systems-mana ger	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associati ons per semplific are l'inventario delle piattaforme e delle applicazioni software all'interno di un'organi zzazione. AWS Syste ms Manager assegna uno stato di configura zione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configura zioni delle applicazi oni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	efs-access-point-e nforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.
4.1	Definizione e mantenimento di un processo di configura zione sicuro	secretsmanager-rot ation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianifica zione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromis sione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizza tiva. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.6	Gestione sicura delle risorse e del software aziendali	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
4.6	Gestione sicura delle risorse e del software aziendali	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.6	Gestione sicura delle risorse e del software aziendali	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
4.6	Gestione sicura delle risorse e del software aziendali	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.6	Gestione sicura delle risorse e del software aziendali	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
4.6	Gestione sicura delle risorse e del software aziendali	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.7	Gestione degli account predefiniti su risorse e software aziendali	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.1	Definizione e mantenimento di un inventario degli account	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Utilizzo di password univoche	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Utilizzo di password univoche	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Utilizzo di password univoche	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Utilizzo di password univoche	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.3	Disattivazione degli account dormienti	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4	Limitazione dei privilegi di amministratore agli account amministratore dedicati	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4	Limitazione dei privilegi di amministratore agli account amministratore dedicati	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.6	Centralizzazione della gestione degli account	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.4	Richiesta di MFA per l'accesso remoto alla rete	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.4	Richiesta di MFA per l'accesso remoto alla rete	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.4	Richiesta di MFA per l'accesso remoto alla rete	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6,5	Richiesta dell'MFA per l'accesso amministrativo	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.7	Centralizzazione del controllo degli accessi	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
7.1	Definizione e mantenimento di un processo di gestione delle vulnerabilità	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1	Definizione e mantenimento di un processo di gestione delle vulnerabilità	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1	Definizione e mantenimento di un processo di gestione delle vulnerabilità	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
7.3	Esecuzione della gestione automatizzata delle patch del sistema operativo	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.3	Esecuzione della gestione automatizzata delle patch del sistema operativo	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.3	Esecuzione della gestione automatizzata delle patch del sistema operativo	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.4	Esecuzione della gestione automatizzata delle patch delle applicazioni	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.4	Esecuzione della gestione automatizzata delle patch delle applicazioni	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.4	Esecuzione della gestione automatizzata delle patch delle applicazioni	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7,5	Esecuzione delle scansioni automatic he di vulnerabilità delle risorse aziendali interne	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilita zione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.
8.1	Definizione e mantenimento di un processo di gestione dei log di audit	audit-log-policy-e xists (Controllo del processo)	Definizione e mantenimento di una policy di gestione dei log di audit che definisca i requisiti di gestione dei log dell'organizzazion e. Ciò include, a titolo esemplificativo, la revisione e la conservazione dei log di audit.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
8.2	Raccolta dei log di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2	Raccolta dei log di audit	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.
8.3	Garanzia di un'adeguata archiviazione dei log di controllo	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.5	Raccolta di log di controllo dettagliati	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8,5	Raccolta di log di controllo dettagliati	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.5	Raccolta di log di controllo dettagliati	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8,5	Raccolta di log di controllo dettagliati	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
8.5	Raccolta di log di controllo dettagliati	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.5	Raccolta di log di controllo dettagliati	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.5	Raccolta di log di controllo dettagliati	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8,5	Raccolta di log di controllo dettagliati	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8,5	Raccolta di log di controllo dettagliati	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8,5	Raccolta di log di controllo dettagliati	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8,5	Raccolta di log di controllo dettagliati	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.5	Raccolta di log di controllo dettagliati	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.5	Raccolta di log di controllo dettagliati	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
8.5	Raccolta di log di controllo dettagliati	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.7	Raccolta di log di controllo delle richieste URL	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
8.9	Centralizzazione dei log di verifica	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.10	Conservazione dei log di audit	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.
8.10	Conservazione dei log di audit	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementazione e gestione di software antimalware	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2	Configurazione degli aggiornamenti automatici delle firme antimalware	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.4	Configurazione della scansione antimalware automatica dei supporti rimovibili	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.6	Gestione centralizzata del software antimalware	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.7	Utilizzo di un software antimalware basato sul comportamento	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
11.2	Esecuzione di backup automatici	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.2	Esecuzione di backup automatici	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
11.2	Esecuzione di backup automatici	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.3	Protezione dei dati di ripristino	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
11.3	Protezione dei dati di ripristino	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
11.3	Protezione dei dati di ripristino	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.3	Protezione dei dati di ripristino	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	acm-certificate-expiration-check	Garantisci che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
12.2	Definizione e mantenimento di un'architettura di rete sicura	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
12.2	Definizione e mantenimento di un'architettura di rete sicura	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS
12.2	Definizione e mantenimento di un'architettura di rete sicura	ec2-instance-no-pu blic-ip	Gestisci l'accesso al AWS cloud assicuran do che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
12.2	Definizione e mantenimento di un'architettura di rete sicura	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
12.2	Definizione e mantenimento di un'architettura di rete sicura	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
12.2	Definizione e mantenimento di un'architettura di rete sicura	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
12.2	Definizione e mantenimento di un'architettura di rete sicura	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
12.2	Definizione e mantenimento di un'architettura di rete sicura	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
12.2	Definizione e mantenimento di un'architettura di rete sicura	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuisce automatic amente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurat i che ELB abbia registrato istanze da più zone di disponibi lità.
12.3	Gestione sicura dell'infrastruttura di rete	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.3	Gestione sicura dell'infrastruttura di rete	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
12.3	Gestione sicura dell'infrastruttura di rete	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.3	Gestione sicura dell'infrastruttura di rete	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
12.3	Gestione sicura dell'infrastruttura di rete	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.3	Gestione sicura dell'infrastruttura di rete	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
12.3	Gestione sicura dell'infrastruttura di rete	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.3	Gestione sicura dell'infrastruttura di rete	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
13.1	Centralizzazione degli avvisi sugli eventi di sicurezza	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
13.1	Centralizzazione degli avvisi sugli eventi di sicurezza	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
13.3	Implementazione di una soluzione di rilevamento delle intrusioni di rete	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
13.6	Raccolta dei log del flusso di traffico di rete	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
13,6	Raccolta dei log del flusso di traffico di rete	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16.1	Definizione e mantenimento di un processo di sviluppo delle applicazioni sicuro	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16.1	Definizione e mantenimento di un processo di sviluppo delle applicazioni sicuro	codebuild-project-source-repo-url-check	Assicurati che l' GitHub URL del repository di origine di Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16.1	Definizione e mantenimento di un processo di sviluppo delle applicazioni sicuro	codebuild-project-environment-privileged-check	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che il tuo ambiente di CodeBuild progetto Amazon non abbia la modalità privilegiata abilitata. Questa impostazione deve essere disabilitata per impedire l'accesso involontario alle API Docker e all'hardware sottostante del container.
16.1	Definizione e mantenimento di un processo di sviluppo delle applicazioni sicuro	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16.1	Definizione e mantenimento di un processo di sviluppo delle applicazioni sicuro	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CIS Critical Security Controls v8 IG2.

Best practice operative per CIS Critical Security Controls v8 IG3

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra Center for Internet Security (CIS) Critical Security Controls v8 IG3 e le regole Config gestite AWS . Ciascuna AWS Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CIS Critical Security Controls v8 IG3. Un

controllo CIS Critical Security Controls v8 IG3 può essere correlato a più regole di AWS Config . Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito,

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			secondo gli standard dell'organizzazione.
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
1.1	Definizione e gestione di un inventario dettagliato delle risorse aziendali	ec2-security-group-attached-to-eni	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambi ente.
2.2	Verifica che il software autorizza to sia attualmente supportato	elastic-beanstalk-managed-updates-en abled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
2.2	Verifica che il software autorizzato sia attualmente supportato	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
2.2	Verifica che il software autorizzato sia attualmente supportato	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribuiti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
2.4	Utilizzo di strumenti automatizzati per l'inventario del software	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
2.4	Utilizzo di strumenti automatizzati per l'inventario del software	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
3.3	Configurazione delle liste di controllo degli accessi	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.3	Configurazione delle liste di controllo degli accessi	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			e altre informazioni amministrative su ogni principale.
3.3	Configurazione delle liste di controllo degli accessi	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.3	Configurazione delle liste di controllo degli accessi	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			riflettere le policy dell'organizzazione.
3.3	Configurazione delle liste di controllo degli accessi	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.3	Configurazione delle liste di controllo degli accessi	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
3.3	Configurazione delle liste di controllo degli accessi	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.3	Configurazione delle liste di controllo degli accessi	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
3.3	Configurazione delle liste di controllo degli accessi	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
3.3	Configurazione delle liste di controllo degli accessi	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegi o minimo, assicurat i che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).
3.3	Configurazione delle liste di controllo degli accessi	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.3	Configurazione delle liste di controllo degli accessi	efs-access-point-enforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.
3.4	Applicazione della conservazione dei dati	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.4	Applicazione della conservazione dei dati	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.
3,10	Crittografia dei dati sensibili in transito	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3,10	Crittografia dei dati sensibili in transito	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
3,10	Crittografia dei dati sensibili in transito	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.10	Crittografia dei dati sensibili in transito	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
3,10	Crittografia dei dati sensibili in transito	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3,10	Crittografia dei dati sensibili in transito	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3,10	Crittografia dei dati sensibili in transito	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.10	Crittografia dei dati sensibili in transito	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
3.10	Crittografia dei dati sensibili in transito	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.10	Crittografia dei dati sensibili in transito	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.11	Crittografia dei dati sensibili a riposo	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.11	Crittografia dei dati sensibili a riposo	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
3,11	Crittografia dei dati sensibili a riposo	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
3,11	Crittografia dei dati sensibili a riposo	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3,11	Crittografia dei dati sensibili a riposo	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
3.11	Crittografia dei dati sensibili a riposo	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.11	Crittografia dei dati sensibili a riposo	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
3.11	Crittografia dei dati sensibili a riposo	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3,11	Crittografia dei dati sensibili a riposo	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
3,11	Crittografia dei dati sensibili a riposo	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3,11	Crittografia dei dati sensibili a riposo	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.11	Crittografia dei dati sensibili a riposo	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
3.11	Crittografia dei dati sensibili a riposo	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.11	Crittografia dei dati sensibili a riposo	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.
3.11	Crittografia dei dati sensibili a riposo	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3,11	Crittografia dei dati sensibili a riposo	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.11	Crittografia dei dati sensibili a riposo	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
3.11	Crittografia dei dati sensibili a riposo	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.14	Log di accesso ai dati sensibili	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3,14	Log di accesso ai dati sensibili	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.14	Log di accesso ai dati sensibili	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3,14	Log di accesso ai dati sensibili	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
3.14	Log di accesso ai dati sensibili	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.14	Log di accesso ai dati sensibili	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.14	Log di accesso ai dati sensibili	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3,14	Log di accesso ai dati sensibili	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3,14	Log di accesso ai dati sensibili	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3,14	Log di accesso ai dati sensibili	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3,14	Log di accesso ai dati sensibili	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.14	Log di accesso ai dati sensibili	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
3.14	Log di accesso ai dati sensibili	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
3.14	Log di accesso ai dati sensibili	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	account-part-of-or ganizations	La gestione centraliz zata Account AWS all'interno di AWS Organizations aiuta a garantire la conformit à degli account. L'assenza di una governance centraliz zata degli account può comportar e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
4.1	Definizione e mantenimento di un processo di configura zione sicuro	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	ec2-volume-inuse-c heck	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	redshift-cluster-m aintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizza zione. In particola re, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il. allowVersionUpgrad e Il valore predefini to è true. Inoltre, consente di impostare facoltativamente il preferredMaintenan ceWindow (l'impost azione predefinita è sab: 16:00 -sab: 16:30) e il automated SnapshotRetention periodo (l'impost azione predefinita è 1). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	ec2-instance-manag ed-by-systems-mana ger	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associati ons per semplific are l'inventario delle piattaforme e delle applicazioni software all'interno di un'organi zzazione. AWS Syste ms Manager assegna uno stato di configura zione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configura zioni delle applicazi oni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	efs-access-point-e nforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.
4.1	Definizione e mantenimento di un processo di configura zione sicuro	secretsmanager-rot ation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianifica zione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromis sione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
4.1	Definizione e mantenimento di un processo di configura zione sicuro	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizza tiva. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
4.6	Gestione sicura delle risorse e del software aziendali	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
4.6	Gestione sicura delle risorse e del software aziendali	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
4.6	Gestione sicura delle risorse e del software aziendali	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
4.6	Gestione sicura delle risorse e del software aziendali	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
4.6	Gestione sicura delle risorse e del software aziendali	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
4.6	Gestione sicura delle risorse e del software aziendali	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
4.7	Gestione degli account predefiniti su risorse e software aziendali	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
5.1	Definizione e mantenimento di un inventario degli account	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
5.2	Utilizzo di password univoche	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
5.2	Utilizzo di password univoche	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
5.2	Utilizzo di password univoche	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
5.2	Utilizzo di password univoche	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
5.3	Disattivazione degli account dormienti	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
5.4	Limitazione dei privilegi di amministratore agli account amministratore dedicati	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
5.4	Limitazione dei privilegi di amministratore agli account amministratore dedicati	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
5.6	Centralizzazione della gestione degli account	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
6.4	Richiesta di MFA per l'accesso remoto alla rete	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
6.4	Richiesta di MFA per l'accesso remoto alla rete	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
6.4	Richiesta di MFA per l'accesso remoto alla rete	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
6,5	Richiesta dell'MFA per l'accesso amministrativo	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
6.7	Centralizzazione del controllo degli accessi	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
7.1	Definizione e mantenimento di un processo di gestione delle vulnerabilità	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
7.1	Definizione e mantenimento di un processo di gestione delle vulnerabilità	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
7.1	Definizione e mantenimento di un processo di gestione delle vulnerabilità	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
7.3	Esecuzione della gestione automatizzata delle patch del sistema operativo	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
7.3	Esecuzione della gestione automatizzata delle patch del sistema operativo	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
7.3	Esecuzione della gestione automatizzata delle patch del sistema operativo	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
7.4	Esecuzione della gestione automatizzata delle patch delle applicazioni	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
7.4	Esecuzione della gestione automatizzata delle patch delle applicazioni	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
7.4	Esecuzione della gestione automatizzata delle patch delle applicazioni	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
7,5	Esecuzione delle scansioni automatic he di vulnerabilità delle risorse aziendali interne	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilita zione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.
8.1	Definizione e mantenimento di un processo di gestione dei log di audit	audit-log-policy-e xists (Controllo del processo)	Definizione e mantenimento di una policy di gestione dei log di audit che definisca i requisiti di gestione dei log dell'organizzazion e. Ciò include, a titolo esemplificativo, la revisione e la conservazione dei log di audit.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.2	Raccolta dei log di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.2	Raccolta dei log di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.2	Raccolta dei log di audit	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.2	Raccolta dei log di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
8.2	Raccolta dei log di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.2	Raccolta dei log di audit	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.2	Raccolta dei log di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.2	Raccolta dei log di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.2	Raccolta dei log di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.2	Raccolta dei log di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.2	Raccolta dei log di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.2	Raccolta dei log di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.2	Raccolta dei log di audit	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.
8.3	Garanzia di un'adeguata archiviazione dei log di controllo	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.5	Raccolta di log di controllo dettagliati	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8,5	Raccolta di log di controllo dettagliati	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.5	Raccolta di log di controllo dettagliati	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8,5	Raccolta di log di controllo dettagliati	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
8.5	Raccolta di log di controllo dettagliati	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.5	Raccolta di log di controllo dettagliati	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.5	Raccolta di log di controllo dettagliati	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8,5	Raccolta di log di controllo dettagliati	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8,5	Raccolta di log di controllo dettagliati	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8,5	Raccolta di log di controllo dettagliati	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8,5	Raccolta di log di controllo dettagliati	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.5	Raccolta di log di controllo dettagliati	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.5	Raccolta di log di controllo dettagliati	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
8.5	Raccolta di log di controllo dettagliati	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.7	Raccolta di log di controllo delle richieste URL	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
8.9	Centralizzazione dei log di verifica	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
8.10	Conservazione dei log di audit	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.
8.10	Conservazione dei log di audit	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
10.1	Implementazione e gestione di software antimalware	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
10.2	Configurazione degli aggiornamenti automatici delle firme antimalware	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
10.4	Configurazione della scansione antimalwa re automatica dei supporti rimovibili	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
10.6	Gestione centralizzata del software antimalware	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
10.7	Utilizzo di un software antimalware basato sul comportamento	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	Esecuzione di backup automatici	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	Esecuzione di backup automatici	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	Esecuzione di backup automatici	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
11.2	Esecuzione di backup automatici	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	Esecuzione di backup automatici	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	Esecuzione di backup automatici	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	Esecuzione di backup automatici	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	Esecuzione di backup automatici	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	Esecuzione di backup automatici	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	Esecuzione di backup automatici	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	Esecuzione di backup automatici	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
11.2	Esecuzione di backup automatici	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Protezione dei dati di ripristino	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
11.3	Protezione dei dati di ripristino	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
11.3	Protezione dei dati di ripristino	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Protezione dei dati di ripristino	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
11.4	Definizione e mantenimento di un'istanza isolata di dati di ripristino	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	acm-certificate-expiration-check	Garantisci che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
12.2	Definizione e mantenimento di un'architettura di rete sicura	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
12.2	Definizione e mantenimento di un'architettura di rete sicura	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS
12.2	Definizione e mantenimento di un'architettura di rete sicura	ec2-instance-no-pu blic-ip	Gestisci l'accesso al AWS cloud assicuran do che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
12.2	Definizione e mantenimento di un'architettura di rete sicura	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
12.2	Definizione e mantenimento di un'architettura di rete sicura	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
12.2	Definizione e mantenimento di un'architettura di rete sicura	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
12.2	Definizione e mantenimento di un'architettura di rete sicura	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
12.2	Definizione e mantenimento di un'architettura di rete sicura	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			e le operazioni del database non appena il failover è completato.
12.2	Definizione e mantenimento di un'architettura di rete sicura	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.2	Definizione e mantenimento di un'architettura di rete sicura	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuisce automatic amente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurat i che ELB abbia registrato istanze da più zone di disponibi lità.
12.3	Gestione sicura dell'infrastruttura di rete	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.3	Gestione sicura dell'infrastruttura di rete	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
12.3	Gestione sicura dell'infrastruttura di rete	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.3	Gestione sicura dell'infrastruttura di rete	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
12.3	Gestione sicura dell'infrastruttura di rete	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.3	Gestione sicura dell'infrastruttura di rete	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
12.3	Gestione sicura dell'infrastruttura di rete	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.3	Gestione sicura dell'infrastruttura di rete	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
12.6	Utilizzo di protocolli di comunicazione e gestione della rete sicuri	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
13.1	Centralizzazione degli avvisi sugli eventi di sicurezza	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
13.1	Centralizzazione degli avvisi sugli eventi di sicurezza	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
13.3	Implementazione di una soluzione di rilevamento delle intrusioni di rete	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
13.6	Raccolta dei log del flusso di traffico di rete	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
13,6	Raccolta dei log del flusso di traffico di rete	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
13.10	Esecuzione del filtraggio a livello di applicazione	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
16.1	Definizione e mantenimento di un processo di sviluppo delle applicazioni sicuro	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
16.1	Definizione e mantenimento di un processo di sviluppo delle applicazioni sicuro	codebuild-project-source-repo-url-check	Assicurati che l' GitHub URL del repository di origine di Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
16.1	Definizione e mantenimento di un processo di sviluppo delle applicazioni sicuro	codebuild-project-environment-privileged-check	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che il tuo ambiente di CodeBuild progetto Amazon non abbia la modalità privilegiata abilitata. Questa impostazione deve essere disabilitata per impedire l'accesso involontario alle API Docker e all'hardware sottostante del container.
16.1	Definizione e mantenimento di un processo di sviluppo delle applicazioni sicuro	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
16.1	Definizione e mantenimento di un processo di sviluppo delle applicazioni sicuro	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
16.12	Implementazione di controlli di sicurezza a livello di codice	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
16.12	Implementazione di controlli di sicurezza a livello di codice	codebuild-project-source-repo-url-check	Assicurati che l' GitHub URL del repository di origine di Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
16.12	Implementazione di controlli di sicurezza a livello di codice	codebuild-project-environment-privileged-check	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che il tuo ambiente di CodeBuild progetto Amazon non abbia la modalità privilegiata abilitata. Questa impostazione deve essere disabilitata per impedire l'accesso involontario alle API Docker e all'hardware sottostante del container.
16.12	Implementazione di controlli di sicurezza a livello di codice	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
16.12	Implementazione di controlli di sicurezza a livello di codice	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CIS Critical Security Controls v8 IG3.

Best practice operative per CIS Top 20

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra i 20 principali controlli di sicurezza critici del Center for Internet Security (CIS) e le regole di AWS Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CIS Top 20. Un controllo CIS Top 20 può

essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo Conformance Pack è stato convalidato da AWS Security Assurance Services LLC (AWS SAS), che è un team di Payment Card Industry Qualified Security Assessors (QSA), HITRUST Certified Common Security Framework Practitioners (ccSFP) e professionisti della conformità certificati per fornire linee guida e valutazioni per vari framework di settore. AWS I professionisti SAS hanno progettato questo Conformance Pack per consentire a un cliente di allinearsi a un sottoinsieme della Top 20 del CIS.

ID controllo	AWS Config Regola	Linea guida
CIS.2	ec2- -controlla managedinstance-association-compliance-status	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.
CIS.2	ec2- -controlla managedinstance-patch-compliance-status	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come

ID controllo	AWS Config Regola	Linea guida
		richiesto dalle politiche e dalle procedure dell'organizzazione.
CIS.2	ec2- -eni security-group-attached-to	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanz a Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambiente.
CIS.2	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) controllando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.2	ec2- volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'elimina zione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata , potrebbe violare il concetto di funzionalità minima.
CIS.2	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	AWS Config Regola	Linea guida
CIS.3	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
CIS.3	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.3	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
CIS.4	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Config Regola	Linea guida
CIS.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
CIS.4	iam-root-access-key-controlla	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Config Regola	Linea guida
CIS.4	root-account-hardware-mfa-abilitato	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
CIS.4	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Config Regola	Linea guida
CIS.4	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
CIS.5	ec2- -manager instance-managed-by-systems	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Config Regola	Linea guida
CIS.5	ec2- -controlla managedinstance-association-compliance-status	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.
CIS.5	ec2- -controlla managedinstance-patch-compliance-status	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.5	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.5	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.
CIS.6	api-gw-execution-logging-abilitato	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	AWS Config Regola	Linea guida
CIS.6	cloud-trail-cloud-watch-abilitato ai registri	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
CIS.6	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Config Regola	Linea guida
CIS.6	cloud-trail-log-file-abilitato alla convalida	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrai l Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
CIS.6	cloudtrail-s3-dataevents-en abled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli Account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indiriz zo IP e l'ora dell'evento.

ID controllo	AWS Config Regola	Linea guida
CIS.6	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	AWS Config Regola	Linea guida
CIS.6	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
CIS.6	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Config Regola	Linea guida
CIS.6	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.6	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail invierà i file di registro da tutti Regioni AWS al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS lanci a una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Config Regola	Linea guida
CIS.6	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.6	s3- bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Config Regola	Linea guida
CIS.6	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
CIS.6	vpc-flow-logs-enabled	I log di flusso VPC forniscon o record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Config Regola	Linea guida
CIS.8	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
CIS.9	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CIS.9	ebs-snapshot-public-restorable-controlla	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Config Regola	Linea guida
CIS.9	ec2- instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CIS.9	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Config Regola	Linea guida
CIS.9	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.
CIS.9	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Config Regola	Linea guida
CIS.9	ec2- instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isola mento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Config Regola	Linea guida
CIS.9	internet-gateway-authorized-vpc-solo	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CIS.9	lambda-function-public-access-proibito	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Config Regola	Linea guida
CIS.9	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Config Regola	Linea guida
CIS.9	rds-instance-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CIS.9	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CIS.9	redshift-cluster-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Config Regola	Linea guida
CIS.9	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.9	blocchi s3 account-level-public-access	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
CIS.9	s3- bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Config Regola	Linea guida
CIS.9	s3- bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CIS.9	sagemaker-notebook-no-direct-accesso a Internet	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
CIS.9	vpc-default-security-group-chiuso	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Config Regola	Linea guida
CIS.9	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
CIS.10	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	AWS Config Regola	Linea guida
CIS.10	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
CIS.10	elasticache-redis-cluster-automatic-controllo del backup	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	AWS Config Regola	Linea guida
CIS.10	s-3 bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
CIS.10	s3- bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.

ID controllo	AWS Config Regola	Linea guida
CIS.11	ec2- -eni security-group-attached-to	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanz a Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambiente.
CIS.11	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Config Regola	Linea guida
CIS.11	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.
CIS.11	vpc-default-security-group-chiuso	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Config Regola	Linea guida
CIS.11	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
CIS.12	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Config Regola	Linea guida
CIS.12	ebs-snapshot-public-restorable-controlla	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CIS.12	ec2- instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Config Regola	Linea guida
CIS.12	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
CIS.12	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Config Regola	Linea guida
CIS.12	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
CIS.12	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Config Regola	Linea guida
CIS.12	ec2- instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isola mento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Config Regola	Linea guida
CIS.12	internet-gateway-authorized-vpc-solo	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CIS.12	lambda-function-public-access-proibito	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Config Regola	Linea guida
CIS.12	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Config Regola	Linea guida
CIS.12	rds-instance-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CIS.12	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CIS.12	redshift-cluster-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Config Regola	Linea guida
CIS.12	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.12	blocchi s3 account-level-public-access	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
CIS.12	s3- bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Config Regola	Linea guida
CIS.12	s3- bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CIS.12	sagemaker-notebook-no-direct-accesso a Internet	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Config Regola	Linea guida
CIS.12	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
CIS.12	vpc-default-security-group-chiuso	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Config Regola	Linea guida
CIS.12	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
CIS.13	acm-certificate-expiration-check	Garantisci che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.13	alb-http-to-https-controllo del reindirizzamento	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittogra fate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
CIS.13	api-gw-cache-enabled-e crittografato	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
CIS.13	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
CIS.13	cloudwatch-log-group-encryp ted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	AWS Config Regola	Linea guida
CIS.13	ec2- ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
CIS.13	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
CIS.13	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
CIS.13	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Config Regola	Linea guida
CIS.13	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
CIS.13	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
CIS.13	kms-cmk-not-scheduled-per la cancellazione	Per proteggere i dati archiviat i, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (KMS).AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	AWS Config Regola	Linea guida
CIS.13	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CIS.13	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Config Regola	Linea guida
CIS.13	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.
CIS.13	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Config Regola	Linea guida
CIS.13	s3- bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
CIS.13	abilitato a s3 bucket-server-side-encryption	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.
CIS.13	s3- bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Config Regola	Linea guida
CIS.13	sagemaker-endpoint-configuration-kms-configurato a chiave	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
CIS.13	sagemaker-notebook-instance-kms-configurato con chiave	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Config Regola	Linea guida
CIS.13	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
CIS.14	acm-certificate-expiration-check	Assicurati che l'integrità della rete sia protetta assicurando che i certificati X509 siano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.14	alb-http-to-https-controllo del reindirizzamento	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittogra fate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
CIS.14	api-gw-cache-enabled-e crittografato	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
CIS.14	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
CIS.14	cloudwatch-log-group-encryp ted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	AWS Config Regola	Linea guida
CIS.14	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicam ente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CIS.14	ebs-snapshot-public-restora ble-controlla	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.
CIS.14	ec2- ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Config Regola	Linea guida
CIS.14	ec2- instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CIS.14	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
CIS.14	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	AWS Config Regola	Linea guida
CIS.14	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Config Regola	Linea guida
CIS.14	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.
CIS.14	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Config Regola	Linea guida
CIS.14	kms-cmk-not-scheduled-per la cancellazione	Per proteggere i dati archiviat i, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (KMS).AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
CIS.14	rds-instance-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
CIS.14	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Config Regola	Linea guida
CIS.14	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CIS.14	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
CIS.14	redshift-cluster-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Config Regola	Linea guida
CIS.14	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CIS.14	blocchi s3 account-level-publ ic-access	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictP ublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.14	s3- bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
CIS.14	s3- bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
CIS.14	s3- bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Config Regola	Linea guida
CIS.14	s3- bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CIS.14	abilitato per s3 bucket-server-side-encryption	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
CIS.14	s3- bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Config Regola	Linea guida
CIS.14	sagemaker-endpoint-configuration-kms-configurato a chiave	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
CIS.14	sagemaker-notebook-instance-kms-configurato con chiave	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Config Regola	Linea guida
CIS.14	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
CIS.16	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.16	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Config Regola	Linea guida
CIS.16	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	AWS Config Regola	Linea guida
CIS.16	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.

ID controllo	AWS Config Regola	Linea guida
CIS.16	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
CIS.16	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.16	iam-password-policy	Le identità e le credenzia li vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfan o o superano i requisiti indicati dal NIST SP 800-63 e dal benchmark Centers for Internet Security (CIS) Foundations per quanto riguarda la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSy mbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best

ID controllo	AWS Config Regola	Linea guida
		Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.
CIS.16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.

ID controllo	AWS Config Regola	Linea guida
CIS.16	iam-root-access-key-controlla	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
CIS.16	iam-user-group-membership-controlla	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.

ID controllo	AWS Config Regola	Linea guida
CIS.16	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richieden do l'autenticazione a più fattori per gli utenti.
CIS.16	iam-user-no-policies-controlla	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibili tà che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Config Regola	Linea guida
CIS.16	iam-user-unused-credentials-controlla	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.16	mfa-enabled-for-iam-accesso alla console	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
CIS.16	root-account-hardware-mfa-a bilitato	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Config Regola	Linea guida
CIS.16	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
CIS.16	secretsmanager-rotation-ena bled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianifica zione regolare può abbreviar e il periodo di attività di un segreto e ridurre potenzial mente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	AWS Config Regola	Linea guida
CIS.16	secretsmanager-scheduled-rotation-success-controlla	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione . La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
CIS.16	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Config Regola	Linea guida
CIS.18	codebuild-project-envvar-awscred-controlla	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.
CIS.18	codebuild-project-source-repo-controllo dell'URL	Assicurati che l' GitHub URL del repository di origine di Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub

ID controllo	AWS Config Regola	Linea guida
CIS.18	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
CIS.18	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	AWS Config Regola	Linea guida
CIS.18	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
CIS.2	ec2- -manager instance-managed-by-systems	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CIS Top 20.

Best practice operative per CISA Cyber Essentials

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra Cyber Essentials (CE) Cyber Essentials (CE) della Cybersecurity & Infrastructure Security Agency (CISA) e le regole Config gestite. AWS Ogni AWS Config regola si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CISA CE. Un controllo CISA CE può essere correlato a più regole. AWS Config Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dipendenti-1	Sviluppo di una cultura della consapevolezza per incoraggiare i dipendenti a fare buone scelte online.	security-awareness -program-exists (controllo di processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organiz zazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dipendenti-2	Individuazione dei rischi come il phishing e la compromissione delle e-mail aziendali .XXXXX.	security-awareness -program-exists (controllo di processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organiz zazione da eventuali violazioni della sicurezza o incidenti.
I tuoi dipendenti-3	Mantenimento della consapevolezza sugli eventi attuali relativi alla sicurezza informatica, sfruttand o le lezioni apprese e gli eventi segnalati per rimanere vigili contro l'attuale ambiente delle minacce e attento alle tendenze nel campo della sicurezza informatica.	security-awareness -program-exists (controllo di processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organiz zazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dipendenti-4	Sfrutta la formazione di base sulla sicurezza informatica per migliorare l'esposizione ai concetti, alla terminologia e alle attività di sicurezza informatica associati all'implementazione delle best practice di sicurezza informatica.	security-awareness-program-exists (controllo di processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.
I tuoi dipendenti-5	Identifica le risorse di formazione disponibili tramite associazioni professionali, istituzioni accademiche, settore privato e fonti governative.	security-awareness-program-exists (controllo di processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-1	Individuazione degli elementi presenti sulla rete. Conserva gli inventari delle risorse hardware e software per sapere cosa è in gioco e cosa è a rischio di attacco.	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
I tuoi sistemi-1	Individuazione degli elementi presenti sulla rete. Conserva gli inventari delle risorse hardware e software per sapere cosa è in gioco e cosa è a rischio di attacco.	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-1	Individuazione degli elementi presenti sulla rete. Conserva gli inventari delle risorse hardware e software per sapere cosa è in gioco e cosa è a rischio di attacco.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-1	Individuazione degli elementi presenti sulla rete. Conserva gli inventari delle risorse hardware e software per sapere cosa è in gioco e cosa è a rischio di attacco.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-1	Individuazione degli elementi presenti sulla rete. Conserva gli inventari delle risorse hardware e software per sapere cosa è in gioco e cosa è a rischio di attacco.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
I tuoi sistemi-1	Individuazione degli elementi presenti sulla rete. Conserva gli inventari delle risorse hardware e software per sapere cosa è in gioco e cosa è a rischio di attacco.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-1	Individuazione degli elementi presenti sulla rete. Conserva gli inventari delle risorse hardware e software per sapere cosa è in gioco e cosa è a rischio di attacco.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-2	Utilizzo degli aggiornamenti automatici per tutti i sistemi operativi e i software di terze parti.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-2	Utilizzo degli aggiornamenti automatici per tutti i sistemi operativi e i software di terze parti.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-2	Utilizzo degli aggiornamenti automatici per tutti i sistemi operativi e i software di terze parti.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sat: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-2	Utilizzo degli aggiornamenti automatici per tutti i sistemi operativi e i software di terze parti.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che vengano ruotate dopo aver raggiunto la fine del periodo di crittografia.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) richiede almeno tre nodi di dati per un'elevata disponibilità e tolleranza ai guasti. L'implementazione di un dominio OpenSearch di servizio con almeno tre nodi di dati garantisce le operazioni del cluster in caso di guasto di un nodo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorar e la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	secretsmanager-secret-periodic-rotation	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione periodica abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto. Il valore predefinito è 90 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	secretsmanager-secret-unused	Se in AWS Secrets Manager sono presenti credenziali inutilizzate, è necessario disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola consente di impostare un valore su unusedForDays (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-3	Implementazione di configurazioni di sicurezza per tutte le risorse hardware e software.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi sistemi-4	Rimozione di hardware e software non supportati o non autorizzati dai sistemi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-1	Individuazione dei soggetti presenti sulla rete. Conserva gli inventari delle connessioni di rete (utenti, fornitori, partner commerciali, ecc.).	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
Ciò che ti circonda-1	Individuazione dei soggetti presenti sulla rete. Conserva gli inventari delle connessioni di rete (utenti, fornitori, partner commerciali, ecc.).	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-1	Individuazione dei soggetti presenti sulla rete. Conserva gli inventari delle connessioni di rete (utenti, fornitori, partner commerciali, ecc.).	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-2	Sfruttamento dell'autenticazione a più fattori per tutti gli utenti, a partire dagli utenti con privilegi, amministrativi e con accesso remoto.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-2	Sfruttamento dell'autenticazione a più fattori per tutti gli utenti, a partire dagli utenti con privilegi, amministrativi e con accesso remoto.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-2	Sfruttamento dell'autenticazione a più fattori per tutti gli utenti, a partire dagli utenti con privilegi, amministrativi e con accesso remoto.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-2	Sfruttamento dell'autenticazione a più fattori per tutti gli utenti, a partire dagli utenti con privilegi, amministrativi e con accesso remoto.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-3	Concedi le autorizzazioni di accesso e di amministrazione in base need-to-know al privilegio minimo.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-3	Concedi le autorizzazioni di accesso e di amministrazione in base al need-to-know privilegio minimo.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-3	Concedi le autorizzazioni di accesso e di amministrazione in base al privilegio minimo. need-to-know	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
Ciò che ti circonda-3	Concedi le autorizzazioni di accesso e di amministrazione in base al privilegio minimo need-to-know .	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-3	Concedi le autorizzazioni di accesso e di amministrazione in base al privilegio minimo need-to-know .	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-3	Concedi le autorizzazioni di accesso e di amministrazione in base al privilegio minimo. need-to-know	secretsmanager-secret-unused	Se in AWS Secrets Manager sono presenti credenziali inutilizzate, è necessario disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola consente di impostare un valore su unusedForDays (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-3	Concedi le autorizzazioni di accesso e di amministrazione in base al need-to-know privilegio minimo.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Ciò che ti circonda-4	Utilizzo di password uniche per tutti gli utenti.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundatio

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			nal Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
I tuoi dati-1	Comprensione delle modalità di protezione dei dati.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti dell'host e del dispositivo e le attività in transito data-at-rest e il comportamento degli utenti.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.
I tuoi dati-2	Scopri cosa succede sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti dell'host e del dispositivo e le attività in transito e relative al comportamento degli utenti. data-at-rest	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti dell'host e del dispositivo e le attività in transito data-at-rest e il comportamento degli utenti.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti dell'host e del dispositivo e le attività in transito data-at-rest e relative al comportamento degli utenti.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti dell'host e del dispositivo e le attività in transito e il comportamento degli utenti data-at-rest .	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	acm-certificate-expiration-check	Assicurati che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito data-at-rest e relative al comportamento degli utenti.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	codebuild-project-source-repo-url-check	Assicurati che l' GitHub URL del repository di origine di Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti dell'host e del dispositivo e le attività in transito e relative al comportam ento degli utenti. data-at-rest	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti dell'host e del dispositivo e le attività in transito data-at-rest e sul comportamento degli utenti.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicaz ione centrale all'inter no di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettaglia te sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito data-at-rest e relative al comportamento degli utenti.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti dell'host e del dispositivo e le attività in transito e relative al comportamento degli utenti data-at-rest .	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito data-at-rest e relative al comportamento degli utenti.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti data-at-rest .	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito data-at-rest e relative al comportamento degli utenti.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti dell'host e del dispositivo e le attività in transito e relative al comportamento degli utenti. data-at-rest	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito data-at-rest e relative al comportamento degli utenti.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito data-at-rest e relative al comportamento degli utenti.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti dell'host e del dispositivo e le attività in transito data-at-rest e il comportamento degli utenti.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti data-at-rest .	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti data-at-rest .	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti data-at-rest .	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa succede sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti data-at-rest .	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito data-at-rest e relative al comportamento degli utenti.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito data-at-rest e relative al comportamento degli utenti.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito data-at-rest e relative al comportamento degli utenti.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti data-at-rest .	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti data-at-rest .	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito data-at-rest e relative al comportamento degli utenti.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti dell'host e del dispositivo e le attività in transito e sul comportamento degli utenti. data-at-rest	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti. data-at-rest	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti data-at-rest .	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli utenti data-at-rest .	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-2	Scopri cosa sta succedendo sulla tua rete. Gestisci i componenti di rete e perimetrali, i componenti di host e dispositivi e le attività in transito e relative al comportamento degli data-at-rest utenti.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-3	Protezione del sistema dei nomi di dominio.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurat i che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionD ays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-4	Definizione di backup automatici regolari e ridondanze dei sistemi chiave.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
I tuoi dati-5	Utilizzo delle protezioni per i backup, tra cui sicurezza fisica, crittografia e copie offline.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
I tuoi dati-5	Utilizzo delle protezioni per i backup, tra cui sicurezza fisica, crittografia e copie offline.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
La tua risposta alle situazioni di crisi-2	Guida allo sviluppo di una struttura di reporting interna per rilevare, comunicare e contenere gli attacchi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
La tua risposta alle situazioni di crisi-2	Guida allo sviluppo di una struttura di reporting interna per rilevare, comunicare e contenere gli attacchi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automaticamente e continuamente il backup dei dati critici e delle configurazioni di sistema.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automatic amente e continuam ente il backup dei dati critici e delle configura zioni di sistema.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automaticamente e continuamente il backup dei dati critici e delle configurazioni di sistema.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automatic amente e continuam ente il backup dei dati critici e delle configura zioni di sistema.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automaticamente e continuamente il backup dei dati critici e delle configurazioni di sistema.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automatic amente e continuam ente il backup dei dati critici e delle configura zioni di sistema.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automatic amente e continuam ente il backup dei dati critici e delle configura zioni di sistema.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automatic amente e continuam ente il backup dei dati critici e delle configura zioni di sistema.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automaticamente e continuamente il backup dei dati critici e delle configurazioni di sistema.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automatic amente e continuam ente il backup dei dati critici e delle configura zioni di sistema.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automaticamente e continuamente il backup dei dati critici e delle configurazioni di sistema.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automaticamente e continuamente il backup dei dati critici e delle configurazioni di sistema.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automaticamente e continuamente il backup dei dati critici e delle configurazioni di sistema.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automatic amente e continuam ente il backup dei dati critici e delle configura zioni di sistema.	backup-recovery-po int-minimum-retent ion-check	Per facilitare i processi di backup dei dati, assicurat i che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionD ays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automatic amente e continuam ente il backup dei dati critici e delle configura zioni di sistema.	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automaticamente e continuamente il backup dei dati critici e delle configurazioni di sistema.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-1	Utilizzo di una soluzione di backup che esegua automaticamente e continuamente il backup dei dati critici e delle configurazioni di sistema.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-2	Richiesta dell'autenticazione a più fattori (MFA) per accedere ai sistemi ogni volta che è possibile. L'autenticazione MFA dovrebbe essere richiesta a tutti gli utenti, ma si può iniziare con gli utenti con privilegi, gli utenti amministrativi e gli utenti con accesso remoto.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-2	Richiesta dell'autenticazione a più fattori (MFA) per accedere ai sistemi ogni volta che è possibile. L'autenticazione MFA dovrebbe essere richiesta a tutti gli utenti, ma si può iniziare con gli utenti con privilegi, gli utenti amministrativi e gli utenti con accesso remoto.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione e alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-2	Richiesta dell'autenticazione a più fattori (MFA) per accedere ai sistemi ogni volta che è possibile. L'autenticazione MFA dovrebbe essere richiesta a tutti gli utenti, ma si può iniziare con gli utenti con privilegi, gli utenti amministrativi e gli utenti con accesso remoto.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-2	Richiesta dell'autenticazione a più fattori (MFA) per accedere ai sistemi ogni volta che è possibile. L'autenticazione MFA dovrebbe essere richiesta a tutti gli utenti, ma si può iniziare con gli utenti con privilegi, gli utenti amministrativi e gli utenti con accesso remoto.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-3	Abilitazione degli aggiornamenti automatici quando possibile. Sostituzione di sistemi operativi, applicazioni e hardware non supportati. Test e distribuzione rapida delle patch.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-3	Abilitazione degli aggiornamenti automatici quando possibile. Sostituzione di sistemi operativi, applicazioni e hardware non supportati. Test e distribuzione rapida delle patch.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-3	Abilitazione degli aggiornamenti automatici quando possibile. Sostituzione di sistemi operativi, applicazioni e hardware non supportati. Test e distribuzione rapida delle patch.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Avvio: le prime cose da fare-3	Abilitazione degli aggiornamenti automatici quando possibile. Sostituzione di sistemi operativi, applicazioni e hardware non supportati. Test e distribuzione rapida delle patch.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sat: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CISA Cyber Essentials.

Best practice operative per Criminal Justice Information Services (CJIS)

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra i requisiti di conformità dei Criminal Justice Information Services (CJIS) e le regole di AWS Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CJIS. Un controllo CJIS può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.2	Formazione sulla sensibilizzazione alla sicurezza	security-awareness -program-exists (Controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organiz zazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.3	Risposta agli eventi imprevisti	response-plan-exists-maintained (Controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti. Disporre di piani di risposta aggiornati e formalmente documentati può aiutare a garantire che il personale addetto all'intervento comprenda ruoli, responsabilità e processi da seguire durante un incidente.
5.3	Risposta agli eventi imprevisti	response-plan-tested (Controllo del processo)	Verifica che i piani di risposta agli incidenti e di ripristino siano testati. Questo può aiutare a capire se il piano sarà efficace in caso di incidente e se è necessario risolvere eventuali lacune o apportare aggiornamenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4	Audit e responsabilità	audit-log-policy-exists (Controllo del processo)	Definizione e mantenimento di una policy di gestione dei log di audit che definisca i requisiti di gestione dei log dell'organizzazione. Ciò include, a titolo esemplificativo, la revisione e la conservazione dei log di audit.
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	codebuild-project-s3-logs-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per AWS CodeBuild i log archiviati in Amazon S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
5.4.1	Eventi e contenuti verificabili (sistemi informativi)	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,4,5	Protezione delle informazioni di audit	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.5	Protezione delle informazioni di audit	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.5	Protezione delle informazioni di audit	codebuild-project-s3-logs-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per AWS CodeBuild i log archiviati in Amazon S3.
5.4.6	Conservazione dei record di audit	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.4.6	Conservazione dei record di audit	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2	Applicazione degli accessi	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2	Applicazione degli accessi	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2	Applicazione degli accessi	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
5.5.2	Applicazione degli accessi	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2	Applicazione degli accessi	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola ti consente di impostare facoltativamente RequireUppercaseCharacters (valore CJIS: falso), RequireLowercaseCharacters (valore CJIS: falso), RequireSymbols (valore CJIS: falso), RequireNumbers (valore CJIS: falso), MinimumPasswordLength (valore CJIS: 8), PasswordReusePrevention (valore CJIS: 10) e MaxPasswordAge (valore CJIS: 90) per

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			la tua IAM Password Policy. I valori effettivi devono riflettere le policy dell'orga nizzazione.
5.5.2	Applicazione degli accessi	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2	Applicazione degli accessi	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2	Applicazione degli accessi	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2	Applicazione degli accessi	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2	Applicazione degli accessi	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2	Applicazione degli accessi	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2	Applicazione degli accessi	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2	Applicazione degli accessi	rds-instance-iam-authentication-enabled	Assicurati che l'autenticazione AWS Identity and Access Management (IAM) sia abilitata sulle istanze di Amazon Relational Database Service (Amazon RDS) per controllare l'accesso a sistemi e asset. In questo modo il traffico di rete da e verso il database viene crittografato utilizzando Secure Sockets Layer (SSL). Non devi archiviare le credenziali dell'utente nel database, perché l'autenticazione è gestita esternamente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2	Applicazione degli accessi	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanism i di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzar e le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2.1	Privilegio minimo	codebuild-project-environment-privileged-check	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che il tuo ambiente di CodeBuild progetto Amazon non abbia la modalità privilegiata abilitata. Questa impostazione deve essere disabilitata per impedire l'accesso involontario alle API Docker e all'hardware sottostante del container.
5.5.2.1	Privilegio minimo	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,52,1	Privilegio minimo	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,52,1	Privilegio minimo	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2.1	Privilegio minimo	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2.1	Privilegio minimo	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2.1	Privilegio minimo	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
5,52,1	Privilegio minimo	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2.1	Privilegio minimo	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.2.1	Privilegio minimo	ecs-containers-non privileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,52,1	Privilegio minimo	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
5,52,1	Privilegio minimo	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,52,1	Privilegio minimo	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,52,1	Privilegio minimo	secretsmanager-secret-unused	Se in AWS Secrets Manager sono presenti credenziali inutilizzate, è necessario disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola consente di impostare un valore su unusedForDays (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.6	Accesso remoto	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.5.6	Accesso remoto	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.6.2.1.1	Password	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola ti consente di impostare facoltativamente RequireUppercaseCharacters (valore CJIS: falso), RequireLowercaseCharacters (valore CJIS: falso), RequireSymbols (valore CJIS: falso), RequireNumbers (valore CJIS: falso), MinimumPasswordLength (valore CJIS: 8), PasswordReusePrevention (valore CJIS: 10) e MaxPasswordAge (valore CJIS: 90) per

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			la tua IAM Password Policy. I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.6.2.2	Autenticazione avanzata	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
56.2.2	Autenticazione avanzata	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.6.2.2	Autenticazione avanzata	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.6.2.2	Autenticazione avanzata	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.6.2.2	Autenticazione avanzata	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.6.3.1	Gestione degli identificatori	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
5,71.1	Funzionalità minima	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
5.7.1.1	Funzionalità minima	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
5,71.1	Funzionalità minima	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
5.7.1.1	Funzionalità minima	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
5.7.1.1	Funzionalità minima	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
5.7.1.1	Funzionalità minima	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.7.1.1	Funzionalità minima	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
5.7.1.1	Funzionalità minima	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
5,10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
5.10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanismi di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzare le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.
5,10	Protezione dei sistemi e delle comunicazioni e integrità delle informazioni	waf-regional-webacl-not-empty	Un ACL Web collegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
5.10.1	Applicazione del flusso di informazioni	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
5.10.1	Applicazione del flusso di informazioni	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
5.10.1	Applicazione del flusso di informazioni	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
5.10.1	Applicazione del flusso di informazioni	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
5.10.1	Applicazione del flusso di informazioni	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
5.10.1	Applicazione del flusso di informazioni	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
5.10.1	Applicazione del flusso di informazioni	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
5.10.1	Applicazione del flusso di informazioni	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1	Applicazione del flusso di informazioni	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.1	Protezione dei confini	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
5,101,1	Protezione dei confini	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.1	Protezione dei confini	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
5.10.1.1	Protezione dei confini	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,101,1	Protezione dei confini	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.1	Protezione dei confini	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.1	Protezione dei confini	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
5.10.1.1	Protezione dei confini	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.1	Protezione dei confini	waf-regional-rule-not-empty	Assicurati che il tuo AWS WAF abbia una regola che non sia vuota. Una regola senza condizioni può comportare un comportamento non intenzionale.
5.10.1.1	Protezione dei confini	waf-regional-rulegroup-not-empty	Assicurati che il tuo AWS WAF abbia un gruppo di regole che non sia vuoto. Un gruppo di regole vuoto potrebbe causare un comportamento indesiderato.
5.10.1.1	Protezione dei confini	waf-regional-webacl-not-empty	Un ACL Web allegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.2	Crittografia	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
5,101.2	Crittografia	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,101.2	Crittografia	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
5,101.2	Crittografia	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
5.10.1.2	Crittografia	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.2	Crittografia	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
5.10.1.2	Crittografia	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.
5.10.1.2	Crittografia	codebuild-project-s3-logs-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per AWS CodeBuild i log archiviati in Amazon S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.2	Crittografia	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
5.10.1.2	Crittografia	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,101.2	Crittografia	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
5,101.2	Crittografia	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.2	Crittografia	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.2	Crittografia	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
5.10.1.2	Crittografia	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.2	Crittografia	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
5,101.2	Crittografia	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
5,101.2	Crittografia	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,101.2	Crittografia	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
5,101.2	Crittografia	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,101.2	Crittografia	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.2	Crittografia	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
5,101.2	Crittografia	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,101.2	Crittografia	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
5,101.2	Crittografia	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,101.2	Crittografia	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
5.10.1.2	Crittografia	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.2	Crittografia	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
5.10.1.2	Crittografia	backup-recovery-po int-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.2	Crittografia	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
5.10.1.2	Crittografia	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.2	Crittografia	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
5.10.1.2	Crittografia	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.3	Strumenti e tecniche di rilevamento delle intrusioni	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.3	Strumenti e tecniche di rilevamento delle intrusioni	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.1.3	Strumenti e tecniche di rilevamento delle intrusioni	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.4.1	Gestione delle patch	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.4.1	Gestione delle patch	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.4.1	Gestione delle patch	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.4.1	Gestione delle patch	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribuiti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.4.1	Gestione delle patch	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5,10,4	Avvisi e avvertimenti di sicurezza	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.4.4	Avvisi e avvertimenti di sicurezza	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5.10.4.4	Avvisi e avvertimenti di sicurezza	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CJIS.

Best practice operative per CMMC – Livello 1

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a

uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra la Cybersecurity Maturity Model Certification (CMMC) Level 1 e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CMMC di livello 1. Un controllo CMMC Livello 1 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito:

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.
AC.1.001	Limitazione dell'acce sso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informati vi).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'acce sso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informati vi).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			riflettere le policy dell'organizzazione.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-waf-enabled	Assicurati che il AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
SI.1.211	Implementazione della protezione da codice dannoso in posizioni appropriate all'interno dei sistemi informativi dell'orga nizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CMMC Level 1.

Best practice operative per CMMC – Livello 2

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra la Cybersecurity Maturity Model Certification (CMMC) Level 2 e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CMMC di livello 2. Un controllo CMMC Livello 2 può essere

correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'acce sso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informati vi).	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	autoscaling-launch -config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	ec2-instance-no-pu blic-ip	Gestisci l'accesso al AWS cloud assicuran do che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicuran do che i nodi master del cluster Amazon EMR non siano accessibili pubblicam ente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearc h Service all'inter no di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessaria per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.2.159	Sviluppo e implementazione di piani d'azione progettati per correggere le carenze e ridurre o eliminare le vulnerabilità nei sistemi dell'organizzazione.	vuln-management-plan-exists (Controllo del processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente. Ciò può includere strumenti di gestione delle vulnerabilità, cadenza di scansione ambientale, ruoli e responsabilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.063	Controllo e monitoraggio del software installato dall'utente.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.063	Controllo e monitoraggio del software installato dall'utente.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.063	Controllo e monitoraggio del software installato dall'utente.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.078	Applicazione di una complessità minima della password e cambio di caratteri quando vengono create nuove password.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.079	Divieto di riutilizzo della password per un determinato numero di generazioni.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	response-plan-exists-maintained (Controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti. Disporre di piani di risposta aggiornati e formalmente documentati può aiutare a garantire che il personale addetto all'intervento comprenda ruoli, responsabilità e processi da seguire durante un incidente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
IR.2.093	Rilevamento e segnalazione di eventi.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
MA.2.113	Richiesta di autenticazione a più fattori per stabilire sessioni di manutenzione non locale tramite connessioni di rete esterne e terminare tali connessioni al termine della manutenzione non locale.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
MA.2.113	Richiesta di autentica zione a più fattori per stabilire sessioni di manutenzione non locale tramite connessioni di rete esterne e terminare tali connessioni al termine della manutenzione non locale.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	vuln-scans-performed (Controllo del processo)	Assicurati che le scansioni delle vulnerabilità vengano eseguite in base ai requisiti di conformità. La cadenza di scansione, gli strumenti utilizzati e l'uso dei risultati devono essere definiti dall'organizzazione.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositivi di rete.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.211	Implementazione della protezione da codice dannoso in posizioni appropriate all'interno dei sistemi informativi dell'orga nizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'organizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CMMC Level 2.

Best practice operative per CMMC – Livello 3

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra la Cybersecurity Maturity Model Certification (CMMC) Level 3 e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CMMC di livello 3. Un controllo CMMC Livello 3 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

> **Note**
>
> A causa delle linee guida provvisorie fornite dal DoD e dall'Organismo di accreditamento CMMC in merito alla reciprocità del FedRAMP per i livelli CMMC 3 - 5, si raccomanda ai clienti di AWS GovCloud utilizzare le regioni (USA) in questo momento per tutti i carichi di lavoro che richiedono la conformità ai livelli CMMC 3 - 5. Per questo motivo, i modelli di pacchetto di conformità per i livelli CMMC 3-5 non sono disponibili all'interno della console dei pacchetti di conformità per evitare confusione. I clienti possono installare in modo indipendente le regole di Config che mappano le linee guida provvisorie per CMMC Level 3-5 (senza un modello di pacchetto di conformità) CloudFormation utilizzando il file YAML di esempio collegato a questo documento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.
AC.1.001	Limitazione dell'acce sso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informati vi).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	autoscaling-launch -config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearc h Service all'inter no di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	acm-certificate-expiration-check	Assicurati che l'integrità della rete sia protetta assicurando che i certificati X509 siano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessaria per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.046	Avviso in caso di errore del processo di registrazione di log di audit.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.046	Avviso in caso di errore del processo di registrazione di log di audit.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU.3.046	Avviso in caso di errore del processo di registrazione di log di audit.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.046	Avviso in caso di errore del processo di registrazione di log di audit.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
AU.3.051	Correlazione dei processi di revisione, analisi e reporting dei record di audit per le indagini e la risposta alle indicazioni di attività illegali, non autorizzate, sospette o insolite.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.051	Correlazione dei processi di revisione, analisi e reporting dei record di audit per le indagini e la risposta alle indicazioni di attività illegali, non autorizzate, sospette o insolite.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.2.159	Sviluppo e implementazione di piani d'azione progettati per correggere le carenze e ridurre o eliminare le vulnerabilità nei sistemi dell'organizzazione.	vuln-management-plan-exists (Controllo del processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente. Ciò può includere strumenti di gestione delle vulnerabilità, cadenza di scansione ambientale, ruoli e responsabilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.3.161	Monitoraggio dei controlli di sicurezza su base continuat iva per garantire la continua efficacia dei controlli.	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.3.161	Monitoraggio dei controlli di sicurezza su base continuat iva per garantire la continua efficacia dei controlli.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.3.161	Monitoraggio dei controlli di sicurezza su base continuat iva per garantire la continua efficacia dei controlli.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.063	Controllo e monitoraggio del software installato dall'utente.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.063	Controllo e monitoraggio del software installato dall'utente.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.063	Controllo e monitoraggio del software installato dall'utente.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.078	Applicazione di una complessità minima della password e cambio di caratteri quando vengono create nuove password.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.079	Divieto di riutilizzo della password per un determinato numero di generazioni.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.083	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.083	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.083	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.083	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.086	Disattivazione degli identificatori dopo un determinato periodo di inattività.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.086	Disattivazione degli identificatori dopo un determinato periodo di inattività.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
IR.2.093	Rilevamento e segnalazione di eventi.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
MA.2.113	Richiesta di autentica zione a più fattori per stabilire sessioni di manutenzione non locale tramite connessioni di rete esterne e terminare tali connessioni al termine della manutenzione non locale.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
MA.2.113	Richiesta di autenticazione a più fattori per stabilire sessioni di manutenzione non locale tramite connessioni di rete esterne e terminare tali connessioni al termine della manutenzione non locale.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'organizzazione.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'organizzazione.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'organizzazione.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'orga nizzazione, periodica mente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositivi di rete.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	acm-certificate-expiration-check	Garantisci che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.187	Definizione e gestione delle chiavi crittografiche per la crittografia impiegata nei sistemi organizzativi.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.
SC.3.187	Definizione e gestione delle chiavi crittografiche per la crittografia impiegata nei sistemi organizzativi.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.211	Implementazione della protezione da codice dannoso in posizioni appropriate all'interno dei sistemi informativi dell'orga nizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
SI.1.213	Esecuzione di scansioni periodiche del sistema informati vo e di scansioni in tempo reale dei file provenienti da fonti esterne, man mano che i file vengono scaricati, aperti o eseguiti.	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilita zione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'organizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CMMC Level 3.

Best practice operative per CMMC – Livello 4

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra la Cybersecurity Maturity Model Certification (CMMC) Level 4 e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CMMC di livello 4. Un controllo CMMC Livello 4 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

> **Note**
>
> A causa delle linee guida provvisorie fornite dal DoD e dall'Organismo di accreditamento CMMC in merito alla reciprocità del FedRAMP per i livelli CMMC 3 - 5, si raccomanda ai clienti di AWS GovCloud utilizzare le regioni (USA) in questo momento per tutti i carichi di lavoro che richiedono la conformità ai livelli CMMC 3 - 5. Per questo motivo, i modelli di pacchetto di conformità per i livelli CMMC 3-5 non sono disponibili all'interno della console dei pacchetti di conformità per evitare confusione. I clienti possono installare in modo indipendente le regole di Config che mappano le linee guida provvisorie per CMMC Level 3-5 (senza un modello di pacchetto di conformità) CloudFormation utilizzando il file YAML di esempio collegato a questo documento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.
AC.1.001	Limitazione dell'acce sso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informati vi).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	ec2-instance-no-pu blic-ip	Gestisci l'accesso al AWS cloud assicuran do che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearc h Service all'inter no di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	acm-certificate-expiration-check	Assicurati che l'integrità della rete sia protetta assicurando che i certificati X509 siano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AM.4.226	Sfrutta la capacità di scoprire e identificare sistemi con attributi di componenti specifici (ad esempio, livello di firmware, tipo di sistema operativo) all'interno del tuo inventario.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AM.4.226	Utilizzate la capacità di scoprire e identific are sistemi con attributi di componenti specifici (ad esempio, livello di firmware, tipo di sistema operativo) all'interno del vostro inventario.	ec2-managedinstanc e-association-comp liance-status-check	Utilizza AWS Systems Manager Associati ons per semplific are l'inventario delle piattaforme e delle applicazioni software all'interno di un'organi zzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo , delle installaz ioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AM.4.226	Utilizzate la capacità di scoprire e identific are sistemi con attributi di componenti specifici (ad esempio, livello di firmware, tipo di sistema operativo) all'interno del vostro inventario.	ec2-managedinstanc e-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	api-gw-execution-l ogging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessaria per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.046	Avviso in caso di errore del processo di registrazione di log di audit.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.046	Avviso in caso di errore del processo di registrazione di log di audit.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU.3.046	Avviso in caso di errore del processo di registrazione di log di audit.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.046	Avviso in caso di errore del processo di registrazione di log di audit.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
AU.3.051	Correlazione dei processi di revisione, analisi e reporting dei record di audit per le indagini e la risposta alle indicazioni di attività illegali, non autorizzate, sospette o insolite.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.051	Correlazione dei processi di revisione, analisi e reporting dei record di audit per le indagini e la risposta alle indicazioni di attività illegali, non autorizzate, sospette o insolite.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.4.053	Automatizzazione dell'analisi dei log di audit per identificare e agire sugli indicatori critici (TTP) e/o sulle attività sospette definite dall'organizzazione.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.4.053	Automatizzazione dell'analisi dei log di audit per identificare e agire sugli indicatori critici (TTP) e/o sulle attività sospette definite dall'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
AU.4.053	Automatizzazione dell'analisi dei log di audit per identificare e agire sugli indicatori critici (TTP) e/o sulle attività sospette definite dall'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.4.053	Automatizzazione dell'analisi dei log di audit per identificare e agire sugli indicatori critici (TTP) e/o sulle attività sospette definite dall'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.4.054	Revisione delle informazioni di audit per l'attività in senso lato, oltre che per l'attività per macchina.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.4.054	Revisione delle informazioni di audit per l'attività in senso lato, oltre che per l'attività per macchina.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.4.054	Revisione delle informazioni di audit per l'attività in senso lato, oltre che per l'attività per macchina.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.3.161	Monitoraggio dei controlli di sicurezza su base continuativa per garantire la continua efficacia dei controlli.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.3.161	Monitoraggio dei controlli di sicurezza su base continuat iva per garantire la continua efficacia dei controlli.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.3.161	Monitoraggio dei controlli di sicurezza su base continuat iva per garantire la continua efficacia dei controlli.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.063	Controllo e monitoraggio del software installato dall'utente.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.063	Controllo e monitoraggio del software installato dall'utente.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.063	Controllo e monitoraggio del software installato dall'utente.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.078	Applicazione di una complessità minima della password e cambio di caratteri quando vengono create nuove password.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.079	Divieto di riutilizzo della password per un determinato numero di generazioni.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.083	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.083	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.083	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.083	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.086	Disattivazione degli identificatori dopo un determinato periodo di inattività.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.086	Disattivazione degli identificatori dopo un determinato periodo di inattività.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
IR.2.093	Rilevamento e segnalazione di eventi.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
MA.2.113	Richiesta di autentica zione a più fattori per stabilire sessioni di manutenzione non locale tramite connessioni di rete esterne e terminare tali connessioni al termine della manutenzione non locale.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
MA.2.113	Richiesta di autenticazione a più fattori per stabilire sessioni di manutenzione non locale tramite connessioni di rete esterne e terminare tali connessioni al termine della manutenzione non locale.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'organizzazione.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'organizzazione.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'organizzazione.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'orga nizzazione, periodica mente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.4.150	Utilizzo delle informazioni sulle minacce per elaborare le architetture di sistema e di sicurezza, la selezione delle soluzioni di sicurezza, il monitoraggio, la caccia alle minacce e le attività di risposta e ripristino.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.4.151	Esecuzione di scansioni per porte non autorizzate disponibili attravers o i confini della rete perimetrale sui confini della rete Internet dell'organizzazione e altri confini definiti dall'organizzazione.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.4.151	Esecuzione di scansioni per porte non autorizzate disponibili attraverso i confini della rete perimetrale sui confini della rete Internet dell'organizzazione e altri confini definiti dall'organizzazione.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.4.151	Esecuzione di scansioni per porte non autorizzate disponibili attravers o i confini della rete perimetrale sui confini della rete Internet dell'organizzazione e altri confini definiti dall'organizzazione.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.4.151	Esecuzione di scansioni per porte non autorizzate disponibili attravers o i confini della rete perimetrale sui confini della rete Internet dell'organizzazione e altri confini definiti dall'organizzazione.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA.4.171	Impostazione e mantenimento di una capacità di caccia alle minacce informatiche per cercare indicatori di compromissione nei sistemi dell'organizzazione e rilevare, tracciare e distruggere le minacce che eludono i controlli esistenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositivi di rete.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	acm-certificate-expiration-check	Garantisci che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.187	Definizione e gestione delle chiavi crittografiche per la crittografia impiegata nei sistemi organizzativi.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.
SC.3.187	Definizione e gestione delle chiavi crittografiche per la crittografia impiegata nei sistemi organizzativi.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.4.199	Utilizzo delle informazioni sulle minacce per bloccare in modo proattivo le richieste DNS che raggiungono domini dannosi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.4.199	Utilizzo delle informazioni sulle minacce per bloccare in modo proattivo le richieste DNS che raggiungono domini dannosi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.4.202	Utilizza meccanismi per analizzare codice e script eseguibili (ad esempio, sandbox) che attraversano i confini della rete Internet o altri limiti definiti dall'orga nizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.211	Implementazione della protezione da codice dannoso in posizioni appropriate all'interno dei sistemi informativi dell'orga nizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
SI.1.213	Esecuzione di scansioni periodiche del sistema informati vo e di scansioni in tempo reale dei file provenienti da fonti esterne, man mano che i file vengono scaricati, aperti o eseguiti.	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilita zione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'organizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.4.221	Utilizzo dei dati sugli indicatori di minaccia relativi alle informazioni e ai sistemi protetti e delle mitigazioni efficaci ottenute da organizzazioni esterne per informare il rilevamento delle intrusioni e la caccia alle minacce.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CMMC Level 4.

Best practice operative per CMMC – Livello 5

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra la Cybersecurity Maturity Model Certification (CMMC) Level 5 e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CMMC di livello 5. Un controllo CMMC Livello 5 può essere

correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

> **Note**
>
> A causa delle linee guida provvisorie fornite dal DoD e dall'Organismo di accreditamento CMMC in merito alla reciprocità del FedRAMP per i livelli CMMC 3 - 5, si raccomanda ai clienti di AWS GovCloud utilizzare le regioni (USA) in questo momento per tutti i carichi di lavoro che richiedono la conformità ai livelli CMMC 3 - 5. Per questo motivo, i modelli di pacchetto di conformità per i livelli CMMC 3-5 non sono disponibili all'interno della console dei pacchetti di conformità per evitare confusione. I clienti possono installare in modo indipendente le regole di Config che mappano le linee guida provvisorie per CMMC Level 3-5 (senza un modello di pacchetto di conformità) CloudFormation utilizzando il file YAML di esempio collegato a questo documento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.
AC.1.001	Limitazione dell'acce sso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informati vi).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.001	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.002	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.1.003	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.007	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.2.008	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.013	Monitoraggio e controllo delle sessioni di accesso remoto.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	autoscaling-launch -config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.2.016	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearc h Service all'inter no di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	acm-certificate-expiration-check	Assicurati che l'integrità della rete sia protetta assicurando che i certificati X509 siano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC.3.014	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.017	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.3.018	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.4.023	Controllo dei flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.5.024	Identificazione e riduzione del rischio associato ai punti di accesso wireless non identificati collegati alla rete.	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AM.4.226	Sfrutta la capacità di scoprire e identificare sistemi con attributi di componenti specifici (ad esempio, livello di firmware, tipo di sistema operativo) all'interno del tuo inventario.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AM.4.226	Utilizzate la capacità di scoprire e identificare sistemi con attributi di componenti specifici (ad esempio, livello di firmware, tipo di sistema operativo) all'interno del vostro inventario.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AM.4.226	Utilizzate la capacità di scoprire e identific are sistemi con attributi di componenti specifici (ad esempio, livello di firmware, tipo di sistema operativo) all'interno del vostro inventario.	ec2-managedinstanc e-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	api-gw-execution-l ogging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.041	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessaria per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.2.042	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.046	Avviso in caso di errore del processo di registrazione di log di audit.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.046	Avviso in caso di errore del processo di registrazione di log di audit.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU.3.046	Avviso in caso di errore del processo di registrazione di log di audit.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.046	Avviso in caso di errore del processo di registrazione di log di audit.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.049	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
AU.3.051	Correlazione dei processi di revisione, analisi e reporting dei record di audit per le indagini e la risposta alle indicazioni di attività illegali, non autorizzate, sospette o insolite.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.3.051	Correlazione dei processi di revisione, analisi e reporting dei record di audit per le indagini e la risposta alle indicazioni di attività illegali, non autorizzate, sospette o insolite.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.4.053	Automatizzazione dell'analisi dei log di audit per identificare e agire sugli indicatori critici (TTP) e/o sulle attività sospette definite dall'organizzazione.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.4.053	Automatizzazione dell'analisi dei log di audit per identificare e agire sugli indicatori critici (TTP) e/o sulle attività sospette definite dall'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
AU.4.053	Automatizzazione dell'analisi dei log di audit per identificare e agire sugli indicatori critici (TTP) e/o sulle attività sospette definite dall'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.4.053	Automatizzazione dell'analisi dei log di audit per identificare e agire sugli indicatori critici (TTP) e/o sulle attività sospette definite dall'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.4.054	Revisione delle informazioni di audit per l'attività in senso lato, oltre che per l'attività per macchina.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.4.054	Revisione delle informazioni di audit per l'attività in senso lato, oltre che per l'attività per macchina.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.4.054	Revisione delle informazioni di audit per l'attività in senso lato, oltre che per l'attività per macchina.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.5.055	Individuazione degli asset che non riportano i log di audit e garanzia di registrazione dei sistemi appropriati definiti dall'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AU.5.055	Individuazione degli asset che non riportano i log di audit e garanzia di registrazione dei sistemi appropriati definiti dall'organizzazione.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.5.055	Individuazione degli asset che non riportano i log di audit e garanzia di registrazione dei sistemi appropriati definiti dall'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
AU.5.055	Individuazione degli asset che non riportano i log di audit e garanzia di registrazione dei sistemi appropriati definiti dall'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.5.055	Individuazione degli asset che non riportano i log di audit e garanzia di registrazione dei sistemi appropriati definiti dall'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.5.055	Individuazione degli asset che non riportano i log di audit e garanzia di registrazione dei sistemi appropriati definiti dall'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.5.055	Individuazione degli asset che non riportano i log di audit e garanzia di registrazione dei sistemi appropriati definiti dall'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.5.055	Individuazione degli asset che non riportano i log di audit e garanzia di registrazione dei sistemi appropriati definiti dall'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.5.055	Individuazione degli asset che non riportano i log di audit e garanzia di registrazione dei sistemi appropriati definiti dall'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.5.055	Individuazione degli asset che non riportano i log di audit e garanzia di registrazione dei sistemi appropriati definiti dall'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.5.055	Individuazione degli asset che non riportano i log di audit e garanzia di registrazione dei sistemi appropriati definiti dall'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.3.161	Monitoraggio dei controlli di sicurezza su base continuativa per garantire la continua efficacia dei controlli.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.3.161	Monitoraggio dei controlli di sicurezza su base continuat iva per garantire la continua efficacia dei controlli.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.3.161	Monitoraggio dei controlli di sicurezza su base continuat iva per garantire la continua efficacia dei controlli.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.061	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.062	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.063	Controllo e monitoraggio del software installato dall'utente.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.063	Controllo e monitoraggio del software installato dall'utente.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.063	Controllo e monitoraggio del software installato dall'utente.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.064	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.2.065	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.3.068	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.5.074	Verifica l'integrità e la correttezza del software fondamentale o essenziale per la sicurezza definito dall'organizzazione (ad esempio, root of trust, verifica formale o firme crittografiche).	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.5.074	Verifica l'integrità e la correttezza del software fondamentale o essenziale per la sicurezza definito dall'organizzazione (ad esempio, root of trust, verifica formale o firme crittografiche).	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.5.074	Verifica l'integrità e la correttezza del software essenziale o fondamentale per la sicurezza definito dall'organizzazione (ad esempio, root of trust, verifica formale o firme crittografiche).	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.5.074	Verifica l'integrità e la correttezza del software essenziale o fondamentale per la sicurezza, come definito dall'orga nizzazione (ad esempio, root of trust, verifica formale o firme crittografiche).	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.076	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.1.077	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.078	Applicazione di una complessità minima della password e cambio di caratteri quando vengono create nuove password.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.079	Divieto di riutilizzo della password per un determinato numero di generazioni.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.2.081	Archiviazione e trasmissione di sole password protette da crittografia.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.083	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.083	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.083	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.083	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.086	Disattivazione degli identificatori dopo un determinato periodo di inattività.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.3.086	Disattivazione degli identificatori dopo un determinato periodo di inattività.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.092	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
IR.2.093	Rilevamento e segnalazione di eventi.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.2.093	Rilevamento e segnalazione di eventi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.5.102	Utilizzo di una combinazione di risposte manuali e automatiche in tempo reale alle attività anomale che corrispondono agli schemi degli incidenti.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.5.102	Utilizzo di una combinazione di risposte manuali e automatiche in tempo reale alle attività anomale che corrispondono agli schemi degli incidenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.5.102	Utilizzo di una combinazione di risposte manuali e automatiche in tempo reale alle attività anomale che corrispondono agli schemi degli incidenti.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.5.102	Utilizzo di una combinazione di risposte manuali e automatiche in tempo reale alle attività anomale che corrispondono agli schemi degli incidenti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
MA.2.113	Richiesta di autentica zione a più fattori per stabilire sessioni di manutenzione non locale tramite connessioni di rete esterne e terminare tali connessioni al termine della manutenzione non locale.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
MA.2.113	Richiesta di autenticazione a più fattori per stabilire sessioni di manutenzione non locale tramite connessioni di rete esterne e terminare tali connessioni al termine della manutenzione non locale.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.137	Backup dei dati eseguiti e testati regolarmente.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.2.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'organizzazione.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'organizzazione.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'orga nizzazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'organizzazione.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.3.139	Esecuzione regolare di backup dei dati completi, esaustivi e resilienti, come definito dall'organizzazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
RE.5.140	Garanzia che le strutture di elaborazi one delle informazioni soddisfino i requisiti di continuità, ridondanz a e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RE.5.140	Garanzia che le strutture di elaborazione delle informazioni soddisfino i requisiti di continuità, ridondanza e disponibilità della sicurezza delle informazioni definiti dall'organizzazione.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.2.142	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.4.150	Utilizzo delle informazioni sulle minacce per elaborare le architetture di sistema e di sicurezza, la selezione delle soluzioni di sicurezza, il monitoraggio, la caccia alle minacce e le attività di risposta e ripristino.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.4.151	Esecuzione di scansioni per porte non autorizzate disponibili attravers o i confini della rete perimetrale sui confini della rete Internet dell'organizzazione e altri confini definiti dall'organizzazione.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.4.151	Esecuzione di scansioni per porte non autorizzate disponibili attravers o i confini della rete perimetrale sui confini della rete Internet dell'organizzazione e altri confini definiti dall'organizzazione.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.4.151	Esecuzione di scansioni per porte non autorizzate disponibili attravers o i confini della rete perimetrale sui confini della rete Internet dell'organizzazione e altri confini definiti dall'organizzazione.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RM.4.151	Esecuzione di scansioni per porte non autorizzate disponibili attravers o i confini della rete perimetrale sui confini della rete Internet dell'organizzazione e altri confini definiti dall'organizzazione.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA.4.171	Impostazione e mantenimento di una capacità di caccia alle minacce informatiche per cercare indicatori di compromissione nei sistemi dell'organizzazione e rilevare, tracciare e distruggere le minacce che eludono i controlli esistenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC.1.175	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.1.175	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositivi di rete.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.2.179	Utilizzo di sessioni crittografate per la gestione dei dispositi vi di rete.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.180	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.182	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	acm-certificate-expiration-check	Garantisci che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.185	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.187	Definizione e gestione delle chiavi crittografiche per la crittografia impiegata nei sistemi organizzativi.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.
SC.3.187	Definizione e gestione delle chiavi crittografiche per la crittografia impiegata nei sistemi organizzativi.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che le chiavi master del cliente (CMK) necessarie non siano pianificate per l'eliminazione in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.3.190	Protezione dell'autenticità delle sessioni di comunicazione.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
SC.3.191	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.4.199	Utilizzo delle informazioni sulle minacce per bloccare in modo proattivo le richieste DNS che raggiungono domini dannosi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.4.199	Utilizzo delle informazioni sulle minacce per bloccare in modo proattivo le richieste DNS che raggiungono domini dannosi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.4.202	Utilizza meccanismi per analizzare codice e script eseguibili (ad esempio, sandbox) che attraversano i confini della rete Internet o altri limiti definiti dall'orga nizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.198	Configurazione dei sistemi di monitoraggio per registrare i pacchetti che passano attraverso i confini della rete Internet dell'organizzazione e altri confini definiti dall'organizzazione.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.198	Configurazione dei sistemi di monitoraggio per registrare i pacchetti che passano attraverso i confini della rete Internet dell'organizzazione e altri confini definiti dall'organizzazione.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.198	Configurazione dei sistemi di monitoraggio per registrare i pacchetti che passano attraverso i confini della rete Internet dell'organizzazione e altri confini definiti dall'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.208	Utilizzo di protezioni di confine definite e personalizzate dall'organizzazione, oltre alle soluzioni disponibili in commercio.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.230	Implementazione della conformità delle porte e dei protocolli.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
SC.5.230	Implementazione della conformità delle porte e dei protocolli.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.230	Implementazione della conformità delle porte e dei protocolli.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
SC.5.230	Implementazione della conformità delle porte e dei protocolli.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.230	Implementazione della conformità delle porte e dei protocolli.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.230	Implementazione della conformità delle porte e dei protocolli.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.230	Implementazione della conformità delle porte e dei protocolli.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.5.230	Implementazione della conformità delle porte e dei protocolli.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.5.230	Implementazione della conformità delle porte e dei protocolli.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.210	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.1.211	Implementazione della protezione da codice dannoso in posizioni appropriate all'interno dei sistemi informativi dell'orga nizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
SI.1.213	Esecuzione di scansioni periodiche del sistema informati vo e di scansioni in tempo reale dei file provenienti da fonti esterne, man mano che i file vengono scaricati, aperti o eseguiti.	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilita zione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.214	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.216	Monitoraggio dei sistemi dell'organizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.2.217	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.4.221	Utilizzo dei dati sugli indicatori di minaccia relativi alle informazioni e ai sistemi protetti e delle mitigazioni efficaci ottenute da organizzazioni esterne per informare il rilevamento delle intrusioni e la caccia alle minacce.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.222	Analisi del comportamento del sistema per rilevare e ridurre l'esecuzione di normali comandi e script di sistema che indicano azioni dannose.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.5.223	Monitoraggio continuo di individui e componenti del sistema per rilevare comportamenti anomali o sospetti.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CMMC Level 5.

Best practice operative per CMMC – Livello 1

I Conformance Pack forniscono un framework di conformità generico progettato per consentire all'utente di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra la Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 1 e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CMMC 2.0 Level 1. Un controllo CMMC 2.0 Livello 1 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			alle policy dell'organizzazione.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicuran do che i nodi master del cluster Amazon EMR non siano accessibili pubblicam ente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicaz ione centrale all'inter no di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettaglia te sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.2	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.2	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.2	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.2	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.2	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.2	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-waf-enabled	Assicurati che il AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L1-3.14.1	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L1-3.14.1	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L1-3.14.1	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L1-3.14.2	Implementazione della protezione da codice dannoso in posizioni appropriate all'interno dei sistemi informativi dell'orga nizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
SI.L1-3.14.5	Esecuzione di scansioni periodiche del sistema informati vo e di scansioni in tempo reale dei file provenienti da fonti esterne, man mano che i file vengono scaricati, aperti o eseguiti.	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilita zione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CMMC 2.0 Level 1.

Best practice operative per CMMC – Livello 2

I Conformance Pack forniscono un framework di conformità generico progettato per consentire all'utente di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra la Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CMMC 2.0 di livello 2. Un controllo CMMC 2.0 Livello 2 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.
AC.L1-3.1.1	Limitazione dell'acce sso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informati vi).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.1	Limitazione dell'accesso al sistema informativo agli utenti autorizzati, ai processi che agiscono per conto degli utenti autorizzati o ai dispositivi (compresi altri sistemi informativi).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.2	Limitazione dell'accesso al sistema informativo ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L1-3.1.20	Verifica e controllo /limitazione delle connessioni ai sistemi informativi esterni e del relativo utilizzo.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	autoscaling-launch -config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.L2-3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.L2-3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.6	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.6	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.6	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.6	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.L2-3.1.6	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.6	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.6	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.L2-3.1.6	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.6	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.L2-3.1.6	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esec uzione di tali funzioni nei log di audit.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.7	Protezione degli utenti senza privilegi dall'esecuzione di funzioni privilegiate e cattura dell'esecuzione di tali funzioni nei log di audit.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AC.L2-3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
AC.L2-3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
AC.L2-3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
AC.L2-3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC.L2-3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC.L2-3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC.L2-3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.1	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AU.L2-3.3.1	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.1	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU.L2-3.3.1	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.1	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.1	Creazione e conservazione di record e di log di audit del sistema nella misura necessaria per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.1	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.1	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizza te.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.1	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.1	Creazione e conservazione di record e di log di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali o non autorizzate.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AU.L2-3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU.L2-3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.4	Avviso in caso di errore del processo di registrazione di log di audit.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.4	Avviso in caso di errore del processo di registrazione di log di audit.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU.L2-3.3.4	Avviso in caso di errore del processo di registrazione di log di audit.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.4	Avviso in caso di errore del processo di registrazione di log di audit.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.5	Correlazione dei processi di revisione, analisi e reporting dei record di audit per le indagini e la risposta alle indicazioni di attività illegali, non autorizzate, sospette o insolite.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.5	Correlazione dei processi di revisione, analisi e reporting dei record di audit per le indagini e la risposta alle indicazioni di attività illegali, non autorizzate, sospette o insolite.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU.L2-3.3.8	Protezione delle informazioni di audit e degli strumenti di registrazione di log di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
CA.L2-3.12.2	Sviluppo e implementazione di piani d'azione progettati per correggere le carenze e ridurre o eliminare le vulnerabilità nei sistemi dell'organizzazione.	vuln-management-plan-exists (Controllo del processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente. Ciò può includere strumenti di gestione delle vulnerabilità, cadenza di scansione ambientale, ruoli e responsabilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.L2-3.12.3	Monitoraggio dei controlli di sicurezza su base continuat iva per garantire la continua efficacia dei controlli.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.L2-3.12.3	Monitoraggio dei controlli di sicurezza su base continuat iva per garantire la continua efficacia dei controlli.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA.L2-3.12.3	Monitoraggio dei controlli di sicurezza su base continuat iva per garantire la continua efficacia dei controlli.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.1	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.1	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
CM.L2-3.4.1	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.1	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.1	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
CM.L2-3.4.2	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.2	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.2	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.2	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.2	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.2	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.2	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.2	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.2	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.2	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.2	Individuazione e applicazione delle impostazioni di configurazione della sicurezza per i prodotti informatici utilizzati nei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.3	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
CM.L2-3.4.3	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.3	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
CM.L2-3.4.3	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.3	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.3	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.3	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.3	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.3	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.3	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.3	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.3	Tracciamento, revisione, approvazione o disapprovazione e log delle modifiche ai sistemi dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.7	Limitazione, disabilitazione o prevenzione dell'utilizzo di programmi, funzioni, porte, protocolli e servizi non essenziali.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.9	Controllo e monitoraggio del software installato dall'utente.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.9	Controllo e monitoraggio del software installato dall'utente.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM.L2-3.4.9	Controllo e monitoraggio del software installato dall'utente.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.1	Individuazione degli utenti del sistema informativo, dei processi che agiscono per conto degli utenti o dei dispositivi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.2	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.2	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.2	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.2	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.2	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L1-3.5.2	Autenticazione (o verifica) dell'identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi informativi dell'organizzazione.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.3	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.3	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.3	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.3	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.6	Disattivazione degli identificatori dopo un determinato periodo di inattività.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.6	Disattivazione degli identificatori dopo un determinato periodo di inattività.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.7	Applicazione di una complessità minima della password e cambio di caratteri quando vengono create nuove password.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.8	Divieto di riutilizzo della password per un determinato numero di generazioni.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA.L2-3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.L2-3.6.1	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.L2-3.6.1	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.L2-3.6.1	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.L2-3.6.1	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR.L2-3.6.3	Verifica della capacità di risposta agli incidenti organizzativi.	response-plan-tested (Controllo del processo)	Verifica che i piani di risposta agli incidenti e di ripristino siano testati. Questo può aiutare a capire se il piano sarà efficace in caso di incidente e se è necessario risolvere eventuali lacune o apportare aggiornamenti.
MA.L2-3.7.5	Richiesta di autenticazione a più fattori per stabilire sessioni di manutenzione non locale tramite connessioni di rete esterne e terminare tali connessioni al termine della manutenzione non locale.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
MA.L2-3.7.5	Richiesta di autentica zione a più fattori per stabilire sessioni di manutenzione non locale tramite connessioni di rete esterne e terminare tali connessioni al termine della manutenzione non locale.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA.L2-3.11.2	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA.L2-3.11.2	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA.L2-3.11.2	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA.L2-3.11.2	Scansione delle vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione, periodicamente e quando vengono identificate nuove vulnerabilità che interessano tali sistemi e applicazioni.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezion e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informati vi dell'organizzazion e) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione e delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L1-3.13.1	Monitoraggio, controllo e protezione delle comunicazioni dell'organizzazione (cioè le informazioni trasmesse o ricevute dai sistemi informativi dell'organizzazione) ai limiti esterni e ai limiti interni chiave dei sistemi informativi.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.4	Prevenzione del trasferimento non autorizzato e non intenzionale di informazioni tramite risorse di sistema condivise.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	acm-certificate-expiration-check	Garantisci che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
SC.L2-3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.L2-3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.L2-3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.L2-3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.L2-3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.10	Definizione e gestione delle chiavi crittografiche per la crittografia impiegata nei sistemi organizzativi.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.
SC.L2-3.13.10	Definizione e gestione delle chiavi crittografiche per la crittografia impiegata nei sistemi organizzativi.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che le chiavi master del cliente (CMK) necessarie non siano pianificate per l'eliminazione in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.15	Protezione dell'autenticità delle sessioni di comunicazione.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.L2-3.13.15	Protezione dell'autenticità delle sessioni di comunicazione.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.15	Protezione dell'autenticità delle sessioni di comunicazione.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC.L2-3.13.15	Protezione dell'autenticità delle sessioni di comunicazione.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.15	Protezione dell'autenticità delle sessioni di comunicazione.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC.L2-3.13.15	Protezione dell'autenticità delle sessioni di comunicazione.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassif ied Information) a riposo.	sagemaker-endpoint -configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassif ied Information) a riposo.	sagemaker-notebook -instance-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
SC.L2-3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L1-3.14.1	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L1-3.14.1	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L1-3.14.1	Identificazione, segnalazione e correzione tempestiva dei difetti delle informazioni e del sistema informativo.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L1-3.14.2	Implementazione della protezione da codice dannoso in posizioni appropriate all'interno dei sistemi informativi dell'orga nizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
SI.L1-3.14.5	Esecuzione di scansioni periodiche del sistema informati vo e di scansioni in tempo reale dei file provenienti da fonti esterne, man mano che i file vengono scaricati, aperti o eseguiti.	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilita zione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.3	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.3	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.3	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.3	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
SI.L2-3.14.3	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.3	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.3	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.3	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.3	Monitoraggio degli avvisi e le segnalazioni di sicurezza del sistema e intervento in risposta.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
SI.L2-3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.6	Monitoraggio dei sistemi dell'organizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
SI.L2-3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
SI.L2-3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI.L2-3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for CMMC 2.0 Level 2.

Best practice operative per servizi di calcolo

Questo pacchetto di conformità contiene AWS Config regole basate su Compute Services. Per ulteriori informazioni, consulta Elaborazione per qualsiasi carico di lavoro. Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle AWS Config regole gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Compute Services.

Best practice operative per la resilienza dei dati

Per un elenco di tutte le regole gestite supportate da AWS Config, vedere Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Data Resiliency.

Best practice operative per servizi di database

Questo pacchetto di conformità contiene AWS Config regole basate su Databases Services. Per ulteriori informazioni, vedere Databases on. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Databases Services.

Best practice operative per data lake e servizi di analisi

Questo pacchetto di conformità contiene AWS Config regole per Data Lakes e Analytics Services. Per ulteriori informazioni, consulta Data Lakes and Analytics on. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Data Lakes and Analytics Services.

Best practice operative per DevOps

Questo pacchetto di conformità contiene AWS Config regole basate sull' DevOps interno. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for DevOps.

Best practice operative per EC2

Questo pacchetto di conformità contiene AWS Config regole basate su EC2. Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle AWS Config regole gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for EC2.

Best practice operative per la crittografia e la gestione delle chiavi

Per un elenco di tutte le regole gestite supportate da AWS Config, vedere Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Best practice operative per la crittografia e la gestione delle chiavi.

Best practice operative per la guida alla cibersicurezza dell'ENISA per le PMI

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra la guida sulla sicurezza informatica dell'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) per le PMI e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a una o più guide ENISA Cybersecurity per i controlli delle PMI. Un controllo della guida ENISA sulla cibersicurezza per le PMI può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo modello di pacchetto di conformità di esempio contiene mappature relative ai controlli adattate dalla guida ENISA sulla cibersicurezza per le PMI. La guida ENISA alla cibersicurezza per

le PMI è disponibile nella Guida alla cibersicurezza per le piccole e medie imprese. 12 azioni per rendere sicure la propria impresa.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: PUBBLICARE POLICY DI CIBERSICUREZZA	in materia di cibersicurezza è necessario delineare regole chiare e specifiche.	security-awareness-program-exists (controllo di processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	disponga di misure di sicurezza adeguate.		
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanismi di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzare le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	elasticsearch-encrypted-at-rest	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i domini Amazon Elasticsearch Service (Amazon ES).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	efs-access-point-enforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	codebuild-project-s3-logs-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per AWS CodeBuild i log archiviati in Amazon S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICU REZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservan o dati personali di residenti nell'UE/S EE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon Elasticse arch Service sia abilitata. ode-to-no de La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1_SVILUPPARE UNA BUONA CULTURA DELLA CIBERSICUREZZA: RICORDARE LA PROTEZIONE DEI DATI	Ai sensi del Regolamento generale sulla protezione dei dati dell'UE1, le PMI che trattano o conservano dati personali di residenti nell'UE/SEE devono garantire l'esistenza di controlli di sicurezza adeguati per proteggere tali dati. Ciò include la garanzia che qualsiasi terza parte che lavori per conto della PMI disponga di misure di sicurezza adeguate.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2_FORNIRE UNA FORMAZIONE ADEGUATA	Offerta regolare di corsi di formazion e sulla consapevo lezza della cibersicu rezza per tutti i dipendenti, per garantire che siano in grado di riconosce re e affrontare le varie minacce in questo ambito. Tali corsi devono essere adattati alle PMI e focalizzati su situazioni reali. Offerta di formazion e specializzata in materia di cibersicu rezza ai responsab ili della gestione della cibersicurezza all'interno dell'azie nda, per garantire che abbiano le capacità e le competenz e necessarie per svolgere il loro lavoro.	security-awareness -program-exists (controllo di processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organiz zazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4_SVILUPPARE UN PIANO DI RISPOSTA AGLI INCIDENTI	Sviluppo di un piano formale di risposta agli incidenti, che contenga linee guida chiare, ruoli e responsabilità documentate per garantire che tutti gli incidenti di sicurezza vengano affrontati in modo tempestivo, professionale e appropriato. Per rispondere rapidamente alle minacce alla sicurezza, esamina gli strumenti in grado di monitorare e creare avvisi quando si verificano attività sospette o violazioni della sicurezza.	response-plan-exists-maintained(controllo di processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5_ACCESSO SICURO AI SISTEMI	Tutti gli utenti devono essere invitati a utilizzar e una passphras e, una raccolta di almeno tre parole comuni randomizz ate combinate in una frase che offre un'ottima combinazi one di semplicità di memorizzazione e sicurezza. Se scegli una password tipica, ricorda che: - Deve essere abbastanza lunga, con caratteri minuscoli e maiuscoli , possibilmente anche numeri e caratteri speciali. - Evita espressioni ovvie come "password", sequenze di lettere o numeri come "abc" o "123". - Non si devono utilizzare informazioni personali disponibi li online. Inoltre, a prescindere dal fatto che si utilizzin o passphrase o password, è bene non	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	riutilizzarle altrove. - Non condividerle con i colleghi. - Abilita l'autenticazione a più fattori. - Utilizza un gestore di password dedicato.		Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5_ACCESSO SICURO AI SISTEMI	Tutti gli utenti devono essere invitati a utilizzar e una passphras e, una raccolta di almeno tre parole comuni randomizz ate combinate in una frase che offre un'ottima combinazi one di semplicità di memorizzazione e sicurezza. Se scegli una password tipica, ricorda che: - Deve essere abbastanza lunga, con caratteri minuscoli e maiuscoli , possibilmente anche numeri e caratteri speciali. - Evita espressioni ovvie come "password", sequenze di lettere o numeri come "abc" o "123". - Non si devono utilizzare informazioni personali disponibi li online. Inoltre, a prescindere dal fatto che si utilizzin o passphrase o password, è bene non	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	riutilizzarle altrove. - Non condividerle con i colleghi. - Abilita l'autenticazione a più fattori. - Utilizza un gestore di password dedicato.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5_ACCESSO SICURO AI SISTEMI	Tutti gli utenti devono essere invitati a utilizzar e una passphras e, una raccolta di almeno tre parole comuni randomizz ate combinate in una frase che offre un'ottima combinazi one di semplicità di memorizzazione e sicurezza. Se scegli una password tipica, ricorda che: - Deve essere abbastanza lunga, con caratteri minuscoli e maiuscoli , possibilmente anche numeri e caratteri speciali. - Evita espressioni ovvie come "password", sequenze di lettere o numeri come "abc" o "123". - Non si devono utilizzare informazioni personali disponibi li online. Inoltre, a prescindere dal fatto che si utilizzin o passphrase o password, è bene non	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	riutilizzarle altrove. - Non condividerle con i colleghi. - Abilita l'autenticazione a più fattori. - Utilizza un gestore di password dedicato.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5_ACCESSO SICURO AI SISTEMI	Tutti gli utenti devono essere invitati a utilizzar e una passphras e, una raccolta di almeno tre parole comuni randomizz ate combinate in una frase che offre un'ottima combinazi one di semplicità di memorizzazione e sicurezza. Se scegli una password tipica, ricorda che: - Deve essere abbastanza lunga, con caratteri minuscoli e maiuscoli , possibilmente anche numeri e caratteri speciali. - Evita espressioni ovvie come "password", sequenze di lettere o numeri come "abc" o "123". - Non si devono utilizzare informazioni personali disponibi li online. Inoltre, a prescindere dal fatto che si utilizzin o passphrase o password, è bene non	root-account-hardw are-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richieden do l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	riutilizzarle altrove. - Non condividerle con i colleghi. - Abilita l'autenticazione a più fattori. - Utilizza un gestore di password dedicato.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5_ACCESSO SICURO AI SISTEMI	Tutti gli utenti devono essere invitati a utilizzar e una passphras e, una raccolta di almeno tre parole comuni randomizz ate combinate in una frase che offre un'ottima combinazi one di semplicità di memorizzazione e sicurezza. Se scegli una password tipica, ricorda che: - Deve essere abbastanza lunga, con caratteri minuscoli e maiuscoli , possibilmente anche numeri e caratteri speciali. - Evita espressioni ovvie come "password", sequenze di lettere o numeri come "abc" o "123". - Non si devono utilizzare informazioni personali disponibi li online. Inoltre, a prescindere dal fatto che si utilizzin o passphrase o password, è bene non	root-account-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richieden do l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	riutilizzarle altrove. - Non condividerle con i colleghi. - Abilita l'autenticazione a più fattori. - Utilizza un gestore di password dedicato.		
6_DISPOSITIVI SICURI: MANTIENI IL SOFTWARE PROTETTO DA PATCH E AGGIORNATO	L'ideale è utilizzare una piattaforma centralizzata per gestire le patch. Si consiglia fortemente alle PMI di: - Aggiornare regolarmente tutto il software. - Attivare gli aggiornamenti automatici ogni qualvolta sia possibile. - Identificare il software e l'hardware che richiedono aggiornamenti manuali. - Prendere in considerazione i dispositivi mobili e IoT.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: MANTIENI IL SOFTWARE PROTETTO DA PATCH E AGGIORNATO	L'ideale è utilizzare una piattaforma centralizzata per gestire le patch. Si consiglia fortemente alle PMI di: - Aggiornare regolarmente tutto il software. - Attivare gli aggiornamenti automatici ogni qualvolta sia possibile. - Identificare il software e l'hardware che richiedono aggiornamenti manuali. - Prendere in considerazione i dispositivi mobili e IoT.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: MANTIENI IL SOFTWARE PROTETTO DA PATCH E AGGIORNATO	L'ideale è utilizzare una piattaforma centralizzata per gestire le patch. Si consiglia fortemente alle PMI di: - Aggiornare regolarmente tutto il software. - Attivare gli aggiornamenti automatici ogni qualvolta sia possibile. - Identificare il software e l'hardware che richiedono aggiornamenti manuali. - Prendere in considerazione i dispositivi mobili e IoT.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: MANTIENI IL SOFTWARE PROTETTO DA PATCH E AGGIORNATO	L'ideale è utilizzar e una piattaforma centralizzata per gestire le patch. Si consiglia fortement e alle PMI di: - Aggiornare regolarme nte tutto il software. - Attivare gli aggiornam enti automatici ogni qualvolta sia possibile . - Identificare il software e l'hardwar e che richiedon o aggiornamenti manuali. - Prendere in considerazione i dispositivi mobili e IoT.	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribuiti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: MANTIENI IL SOFTWARE PROTETTO DA PATCH E AGGIORNATO	L'ideale è utilizzare una piattaforma centralizzata per gestire le patch. Si consiglia fortemente alle PMI di: - Aggiornare regolarmente tutto il software. - Attivare gli aggiornamenti automatici ogni qualvolta sia possibile. - Identificare il software e l'hardware che richiedono aggiornamenti manuali. - Prendere in considerazione i dispositivi mobili e IoT.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: MANTIENI IL SOFTWARE PROTETTO DA PATCH E AGGIORNATO	L'ideale è utilizzare una piattaforma centralizzata per gestire le patch. Si consiglia fortemente alle PMI di: - Aggiornare regolarmente tutto il software. - Attivare gli aggiornamenti automatici ogni qualvolta sia possibile. - Identificare il software e l'hardware che richiedono aggiornamenti manuali. - Prendere in considerazione i dispositivi mobili e IoT.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: MANTIENI IL SOFTWARE PROTETTO DA PATCH E AGGIORNATO	L'ideale è utilizzare una piattaforma centralizzata per gestire le patch. Si consiglia fortemente alle PMI di: - Aggiornare regolarmente tutto il software. - Attivare gli aggiornamenti automatici ogni qualvolta sia possibile. - Identificare il software e l'hardware che richiedono aggiornamenti manuali. - Prendere in considerazione i dispositivi mobili e IoT.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei registri. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi artefatti. AWS CodeBuild

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	codebuild-project-s3-logs-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per AWS CodeBuild i log archiviati in Amazon S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	elasticsearch-encrypted-at-rest	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i domini Amazon Elasticsearch Service (Amazon ES).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon Elasticsearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come WiFi reti di hotel o aeroporti, assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6_DISPOSITIVI SICURI: CRITTOGRAFIA	Proteggi i dati crittografandoli. Le PMI devono garantire che i dati memorizzati su dispositivi mobili come laptop, smartphone e tablet siano crittografati. Per i dati trasferiti su reti pubbliche, come reti di hotel o aeroporti WiFi , assicurati che i dati siano crittografati, utilizzando una rete privata virtuale (VPN) o accedendo ai siti Web tramite connessioni sicure utilizzando il protocollo SSL/TLS. I siti web devono utilizzare una tecnologia di crittografia adeguata per proteggere i dati dei clienti quando transitano su Internet.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA RETE UTILIZZANDO I FIREWALL	I firewall gestiscono il traffico in entrata e in uscita da una rete e sono uno strumento fondamentale per proteggere i sistemi delle PMI. I firewall devono essere installati per proteggere tutti i sistemi critici, in particolare per proteggere la rete delle PMI da Internet.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA RETE UTILIZZANDO I FIREWALL	I firewall gestiscono il traffico in entrata e in uscita da una rete e sono uno strumento fondamentale per proteggere i sistemi delle PMI. I firewall devono essere installati per proteggere tutti i sistemi critici, in particolare per proteggere la rete delle PMI da Internet.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA RETE UTILIZZANDO I FIREWALL	I firewall gestiscono il traffico in entrata e in uscita da una rete e sono uno strumento fondamentale per proteggere i sistemi delle PMI. I firewall devono essere installati per proteggere tutti i sistemi critici, in particolare per proteggere la rete delle PMI da Internet.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA RETE UTILIZZANDO I FIREWALL	I firewall gestiscono il traffico in entrata e in uscita da una rete e sono uno strumento fondamentale per proteggere i sistemi delle PMI. I firewall devono essere installati per proteggere tutti i sistemi critici, in particolare per proteggere la rete delle PMI da Internet.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA RETE UTILIZZANDO I FIREWALL	I firewall gestiscono il traffico in entrata e in uscita da una rete e sono uno strumento fondamentale per proteggere i sistemi delle PMI. I firewall devono essere installati per proteggere tutti i sistemi critici, in particolare per proteggere la rete delle PMI da Internet.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA RETE UTILIZZANDO I FIREWALL	I firewall gestiscono il traffico in entrata e in uscita da una rete e sono uno strumento fondamentale per proteggere i sistemi delle PMI. I firewall devono essere installati per proteggere tutti i sistemi critici, in particolare per proteggere la rete delle PMI da Internet.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
7_PROTEGGERE LA RETE UTILIZZANDO I FIREWALL	I firewall gestiscono il traffico in entrata e in uscita da una rete e sono uno strumento fondamentale per proteggere i sistemi delle PMI. I firewall devono essere installati per proteggere tutti i sistemi critici, in particolare per proteggere la rete delle PMI da Internet.	netfw-policy-rule-group-associated	Una policy AWS Network Firewall definisce il modo in cui il firewall monitora e gestisce il traffico in un Amazon VPC. Puoi configurare gruppi di regole stateless e stateful per filtrare pacchetti e flussi di traffico, nonché definire la gestione del traffico predefinita.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA RETE UTILIZZANDO I FIREWALL	I firewall gestiscono il traffico in entrata e in uscita da una rete e sono uno strumento fondamentale per proteggere i sistemi delle PMI. I firewall devono essere installati per proteggere tutti i sistemi critici, in particolare per proteggere la rete delle PMI da Internet.	netfw-stateless-rule-group-not-empty	Un gruppo di regole AWS Network Firewall contiene regole che definiscono il modo in cui il firewall elabora il traffico nel tuo VPC. Un gruppo di regole stateless vuoto, se presente in una policy firewall, non elabora il traffico.
7_PROTEGGERE LA RETE UTILIZZANDO I FIREWALL	I firewall gestiscono il traffico in entrata e in uscita da una rete e sono uno strumento fondamentale per proteggere i sistemi delle PMI. I firewall devono essere installati per proteggere tutti i sistemi critici, in particolare per proteggere la rete delle PMI da Internet.	waf-regional-rule-not-empty	Assicurati che il tuo AWS WAF abbia una regola che non sia vuota. Una regola senza condizioni può comportare un comportamento non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA RETE UTILIZZANDO I FIREWALL	I firewall gestiscono il traffico in entrata e in uscita da una rete e sono uno strumento fondamentale per proteggere i sistemi delle PMI. I firewall devono essere installati per proteggere tutti i sistemi critici, in particolare per proteggere la rete delle PMI da Internet.	waf-regional-rulegroup-not-empty	Assicurati che il tuo AWS WAF abbia un gruppo di regole che non sia vuoto. Un gruppo di regole vuoto potrebbe causare un comportamento indesiderato.
7_PROTEGGERE LA RETE UTILIZZANDO I FIREWALL	I firewall gestiscono il traffico in entrata e in uscita da una rete e sono uno strumento fondamentale per proteggere i sistemi delle PMI. I firewall devono essere installati per proteggere tutti i sistemi critici, in particolare per proteggere la rete delle PMI da Internet.	waf-regional-webacl-not-empty	Un ACL Web allegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini del servizio Amazon Elasticsearch abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di gestione e le chiamate API. AWS È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7_PROTEGGERE LA TUA RETE ESAMINANDO LE SOLUZIONI DI ACCESSO REMOTO	Le PMI devono rivedere regolarmente tutti gli strumenti di accesso remoto per garantirne la sicurezza, in particolare: - Assicurarsi che tutti i software di accesso remoto abbiano le patch necessarie e siano aggiornati. - Limitare l'accesso remoto da posizioni geografiche sospette o da determinati indirizzi IP. - Limitare l'accesso remoto del personale solo ai sistemi e ai computer necessari per lavorare. - Implementare password complesse per l'accesso remoto e, ove possibile, abilitare l'autenticazione a più fattori. - Assicurarsi che il monitoraggio e gli avvisi siano abilitati per segnalare attacchi sospetti o attività insolite sospette.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	backup-plan-min-fr equency-and-min-re tention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservaz ione minime. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredF requencyValue (Config default: 1), (requiredRetentionD ays Config default: 35) e (requiredF requencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurat i che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionD ays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	dynamodb-pitr-enab led	Abilita questa regola per verificare che sia stato eseguito il backup delle informazi oni. Inoltre, mantiene i backup assicuran do che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristin o mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	ec2-resources-prot ected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	fsx-resources-prot ected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	rds-resources-prot ected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	redshift-backup-en abled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatiz zati. Quando gli snapshot automatic i sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazi one predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9_BACKUP SICURI	Per consentire il ripristino della formazione chiave, è necessario mantenere i backup, che rappresentano un modo efficace per ripristinare lo stato precedente un disastro come un attacco ransomwar e. Si consiglia di applicare le seguenti regole di backup: - il backup è regolare e automatizzato quando possibile, - il backup è conservato separatam ente dall'ambiente di produzione della PMI, - i backup sono criptati, soprattutto se devono essere spostati da una sede all'altra, - la capacità di ripristin are regolarmente i dati dai backup è testata. L'ideale sarebbe eseguire un test regolare di un ripristino completo dall'inizio alla fine.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11_SITI ONLINE SICURI	È essenziale che le PMI garantiscano che i loro siti web online siano configurati e gestiti in modo sicuro e che tutti i dati personali o finanziari, come i dati delle carte di credito, siano adeguatamente protetti. Ciò comporterà l'esecuzione di test di sicurezza regolari sui siti web per identificare eventuali punti deboli della sicurezza e l'esecuzione di revisioni regolari per garantire che il sito sia mantenuto e aggiornato correttamente.	vuln-management-plan-exists(controllo di processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente.

Modello

Il modello è disponibile su GitHub: Guida alle migliori pratiche operative per la sicurezza informatica dell'ENISA per le PMI.

Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello basso

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra i controlli del framework low framework spagnolo Esquema Nacional de Seguridad (ENS) e le regole Config gestite. AWS Ogni regola di configurazione si applica a una risorsa AWS specifica e si riferisce a uno o più controlli ENS Low in Spagna. Un controllo ENS in Spagna può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo modello di pacchetto di conformità di esempio contiene mappature ai controlli all'interno del framework ENS Low in Spagna, con ultimo aggiornamento recante data 23/10/2020.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
Allegato II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon

ID controllo	AWS Regola di configurazione	Linea guida
		EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalen ti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
Allegato II 4.1.2.a); b); c)	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	s3-default-encryption-kms	Assicurati che la crittogra fia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittogra fia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	sagemaker-notebook-instance -kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentir e ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Allegato II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
Allegato II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
Allegato II 4.1.2.a); b); c)	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
Allegato II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
Allegato II 4.1.2.a); b); c)	elb-deletion-protection-ena bled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzion almente, con conseguente perdita di disponibilità delle applicazioni.
Allegato II 4.1.2.a); b); c)	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
Allegato II 4.1.2.a); b); c)	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	sagemaker-endpoint-configur ation-kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	secretsmanager-using-cmk	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.
Allegato II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanz a Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.
Allegato II 4.1.2.b)	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'elimina zione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata , potrebbe violare il concetto di funzionalità minima.
Allegato II 4.1.2.b)	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	vpc-network-acl-unused-check	Questa regola garantisc e che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.
Allegato II 4.2.1.a)	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.1.a); b)	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
Allegato II 4.2.4	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.4	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
Allegato II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.4	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
Allegato II 4.2.5	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.3.BAJO.a)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
Allegato II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
Allegato II 4.2.6.BAJO.c)	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
Allegato II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
Allegato II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
Allegato II 4.2.6.BAJO.c)	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Allegato II 4.2.6.BAJO.c)	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	I log di flusso VPC forniscon o record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
Allegato II 4.2.7.BAJO	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.7.BAJO	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
Allegato II 4.2.7.BAJO	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.7.BAJO	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
Allegato II 4.3.1	ec2-managedinstance-associa tion-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazi oni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configura zioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.1	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.
Allegato II 4.3.1	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'elimina zione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata , potrebbe violare il concetto di funzionalità minima.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.1	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
Allegato II 4.3.1	vpc-network-acl-unused-check	Questa regola garantisc e che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
Allegato II 4.1.2.b)	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
Allegato II 4.1.2.b)	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
Allegato II 4.1.2.b)	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
Allegato II 4.1.2.b)	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
Allegato II 4.1.2.b)	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
Allegato II 4.1.2.b)	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
Allegato II 4.1.2.b)	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
Allegato II 4.1.2.b)	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
Allegato II 4.1.2.b)	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
Allegato II 4.1.2.b)	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Allegato II 4.1.2.b)	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Allegato II 4.1.2.b)	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
Allegato II 4.1.2.b)	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
Allegato II 4.3.4.c)	vuln-management-plan-exists (Controllo del processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente. Ciò può includere strumenti di gestione delle vulnerabilità, cadenza di scansione ambientale, ruoli e responsabilità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
Allegato II 4.3.8.BAJO	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
Allegato II 4.3.8.BAJO	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
Allegato II 4.3.8.BAJO	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
Allegato II 4.3.8.BAJO	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Allegato II 4.3.8.BAJO	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	vpc-flow-logs-enabled	I log di flusso VPC forniscon o record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
Allegato II 4.3.10.b)	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i percorsi. AWS CloudTrail

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.10.b)	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
Allegato II 4.3.10.d)	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
Allegato II 4.6.2.BASICA	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.2.3	security-awareness-program-exists (Controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5,4.3.BAJO.a)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
Allegato II 5.6.1.c)	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.
Allegato II 5.6.1.c)	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
Allegato II 5.7.3	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 5.7.3	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
Allegato II 5.7.3	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
Allegato II 5.7.3	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Allegato II 5.7.3	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
Allegato II 5.7.3	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
Allegato II 5.7.3	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
Allegato II 5.7.3	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
Allegato II 5.7.3	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
Allegato II 5.7.3	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 5.7.3	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 5.7.3	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	sagemaker-endpoint-configur ation-kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 5.7.3	secretsmanager-using-cmk	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.4	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.
Allegato II 5.7.4	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
Allegato II 5.8.2	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.2	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
Art. 14.4	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 16	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.
Art. 16	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
Art. 16	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 20.2	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
Art. 20.2	vuln-management-plan-exists (Controllo del processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente. Ciò può includere strumenti di gestione delle vulnerabilità, cadenza di scansione ambientale, ruoli e responsabilità.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
Art. 21.1	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Art. 21.1	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.
Art. 21.1	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
Art. 21.1	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
Art. 21.1	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Art. 21.1	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
Art. 21.1	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Art. 21.1	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
Art. 21.1	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
Art. 21.1	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
Art. 21.1	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
Art. 21.1	elb-deletion-protection-ena bled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzion almente, con conseguente perdita di disponibilità delle applicazioni.
Art. 21.1	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
Art. 21.1	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Art. 21.1	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Art. 21.1	sagemaker-endpoint-configur ation-kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	secretsmanager-using-cmk	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.
Art. 22	autoscaling-launch-config-p ublic-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicam ente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
Art. 22	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
Art. 22	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicam ente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
Art. 22	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
Art. 22	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
Art. 22	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
Art. 22	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
Art. 22	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
Art. 22	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Art. 22	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Art. 22	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
Art. 22	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
Art. 23	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
Art. 23	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
Art. 23	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
Art. 23	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
Art. 23	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Art. 23	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	vpc-flow-logs-enabled	I log di flusso VPC forniscon o record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
Art. 25	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
Art. 25	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
Art. 25	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
Art. 25	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
Art. 25	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
Art. 25	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low.

Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello medio

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra i controlli del framework Medium dell'Esquema Nacional de Seguridad (ENS) in Spagna e le regole Config gestite. AWS Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli Spain ENS Medium. Un controllo ENS in Spagna può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo modello di pacchetto di conformità di esempio contiene mappature ai controlli all'interno del framework ENS Medium in Spagna, con ultimo aggiornamento recante data 23/10/2020.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
Allegato II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon

ID controllo	AWS Regola di configurazione	Linea guida
		EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalen ti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
Allegato II 4.1.2.a); b); c)	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	s3-default-encryption-kms	Assicurati che la crittogra fia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittogra fia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	sagemaker-notebook-instance -kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentir e ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Allegato II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
Allegato II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
Allegato II 4.1.2.a); b); c)	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
Allegato II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
Allegato II 4.1.2.a); b); c)	elb-deletion-protection-ena bled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzion almente, con conseguente perdita di disponibilità delle applicazioni.
Allegato II 4.1.2.a); b); c)	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
Allegato II 4.1.2.a); b); c)	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	sagemaker-endpoint-configur ation-kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	secretsmanager-using-cmk	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.
Allegato II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanz a Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.
Allegato II 4.1.2.b)	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'elimina zione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata , potrebbe violare il concetto di funzionalità minima.
Allegato II 4.1.2.b)	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	vpc-network-acl-unused-check	Questa regola garantisc e che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.
Allegato II 4.2.1.a)	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.1.a); 4.2.1.b)	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
Allegato II 4.2.4	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.4	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
Allegato II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.4	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
Allegato II 4.2.5	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.5.a)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.5.c)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
Allegato II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Allegato II 4.2.6.c)	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.c)	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.c)	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
Allegato II 4.2.6.c)	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.c)	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
Allegato II 4.2.6.c)	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
Allegato II 4.2.6.c)	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.c)	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
Allegato II 4.2.6.c)	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.c)	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
Allegato II 4.2.6.c)	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.7	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
Allegato II 4.2.7	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.7	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
Allegato II 4.2.7	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.1	ec2-security-group-attached-to-eni-periodic	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanz a Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambiente.
Allegato II 4.3.1	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazi oni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configura zioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.1	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.
Allegato II 4.3.1	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'elimina zione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata , potrebbe violare il concetto di funzionalità minima.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.1	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
Allegato II 4.3.1	vpc-network-acl-unused-check	Questa regola garantisc e che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
Allegato II 4.1.2.b)	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
Allegato II 4.1.2.b)	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
Allegato II 4.1.2.b)	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicam ente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
Allegato II 4.1.2.b)	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
Allegato II 4.1.2.b)	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
Allegato II 4.1.2.b)	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
Allegato II 4.1.2.b)	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
Allegato II 4.1.2.b)	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
Allegato II 4.1.2.b)	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
Allegato II 4.1.2.b)	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Allegato II 4.1.2.b)	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Allegato II 4.1.2.b)	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
Allegato II 4.1.2.b)	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
Allegato II 4.3.4.c)	vuln-management-plan-exists (Controllo del processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente. Ciò può includere strumenti di gestione delle vulnerabilità, cadenza di scansione ambientale, ruoli e responsabilità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
Allegato II 4.3.7.a)	response-plan-exists-mainta ined (Controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti. Disporre di piani di risposta aggiornat i e formalmente documenta ti può aiutare a garantire che il personale addetto all'intervento comprenda ruoli, responsabilità e processi da seguire durante un incidente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
Allegato II 4.3.8	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
Allegato II 4.3.8	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
Allegato II 4.3.8	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
Allegato II 4.3.8	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
Allegato II 4.3.8	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Allegato II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Allegato II 4.3.10.b)	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i percorsi. AWS CloudTrail

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.10.b)	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
Allegato II 4.3.10.d)	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
Allegato II 4.6.2	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.6.2	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
Allegato II 5.2.3	security-awareness-program-exists (Controllo del processo)	Definizione e mantenimento di un programma di sensibili zzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.2	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 5.4.2	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
Allegato II 5.4.2	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.2	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.4.2	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Allegato II 5.4.2	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.2	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.4.2	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.3	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 5.4.3	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
Allegato II 5.4.3	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.3	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.4.3	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Allegato II 5.4.3	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.3	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.4.3	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 5.4.3.MEDIO	opensearch-logs-to-cloudwat ch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.3.a)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundatio nal Security Best Practices value: true), RequireSy mbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
Allegato II 5.6.1.c)	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.
Allegato II 5.6.1.c)	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
Allegato II 5.7.3	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 5.7.3	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
Allegato II 5.7.3	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
Allegato II 5.7.3	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Allegato II 5.7.3	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
Allegato II 5.7.3	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
Allegato II 5.7.3	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
Allegato II 5.7.3	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
Allegato II 5.7.3	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
Allegato II 5.7.3	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 5.7.3	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 5.7.3	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	sagemaker-endpoint-configur ation-kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
Allegato II 5.7.3	secretsmanager-using-cmk	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.4	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.
Allegato II 5.7.4	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
Allegato II 5.8.2	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.2	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
Allegato II 5.8.3.b)	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.3.b)	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
Allegato II 5.8.3.b)	elb-cross-zone-load-balanci ng-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalen ti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.3.b)	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
Allegato II 5.8.3.b)	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.3.b)	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.3.b)	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.3.b)	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.
Art. 14.4	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 16	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.
Art. 16	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
Art. 16	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 20.2	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
Art. 20.2	vuln-management-plan-exists (Controllo del processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente. Ciò può includere strumenti di gestione delle vulnerabilità, cadenza di scansione ambientale, ruoli e responsabilità.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
Art. 21.1	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Art. 21.1	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.
Art. 21.1	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
Art. 21.1	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
Art. 21.1	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Art. 21.1	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
Art. 21.1	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Art. 21.1	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
Art. 21.1	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
Art. 21.1	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
Art. 21.1	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
Art. 21.1	elb-deletion-protection-ena bled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzion almente, con conseguente perdita di disponibilità delle applicazioni.
Art. 21.1	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
Art. 21.1	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Art. 21.1	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Art. 21.1	sagemaker-endpoint-configur ation-kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
Art. 21.1	secretsmanager-using-cmk	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.
Art. 22	autoscaling-launch-config-p ublic-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicam ente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
Art. 22	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicam ente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
Art. 22	ebs-snapshot-public-restora ble-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
Art. 22	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.
Art. 22	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
Art. 22	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
Art. 22	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
Art. 22	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
Art. 22	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Art. 22	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Art. 22	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
Art. 22	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
Art. 23	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
Art. 23	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
Art. 23	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
Art. 23	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
Art. 23	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Art. 23	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	vpc-flow-logs-enabled	I log di flusso VPC forniscon o record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
Art. 24.1	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 24.2	response-plan-exists-mainta ined (Controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti. Disporre di piani di risposta aggiornat i e formalmente documenta ti può aiutare a garantire che il personale addetto all'intervento comprenda ruoli, responsabilità e processi da seguire durante un incidente.
Art. 25	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
Art. 25	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
Art. 25	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
Art. 25	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
Art. 25	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
Art. 25	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium.

Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello alto

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra i controlli del framework elevato dell'Esquema Nacional de Seguridad (ENS) in Spagna e le regole Config gestite. AWS Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli Spain ENS High. Un controllo ENS in Spagna può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo modello di pacchetto di conformità di esempio contiene mappature ai controlli all'interno del framework ENS di livello elevato in Spagna, con ultimo aggiornamento recante data 09/07/2021.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.1.ALTO	annual-risk-assessment-performed (Controllo del processo)	Esegui una valutazione annuale del rischio sulla tua organizzazione. Le valutazioni del rischio possono aiutare a determinare la probabilità e l'impatto dei rischi e/o delle vulnerabilità identificati che interessano un'organizzazione.
4.2.1.b)	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management

ID controllo	AWS Regola di configurazione	Linea guida
		(IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
4.2.5.ALTO.a)	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
Allegato II 4.1.2.a); b); c)	dynamodb-table-encrypted-km s	Assicurati che la crittogra fia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefini ta, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.
Allegato II 4.1.2.a); b); c)	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	s3-default-encryption-kms	Assicurati che la crittogra fia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittogra fia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
Allegato II 4.1.2.a); b); c)	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Allegato II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
Allegato II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
Allegato II 4.1.2.a); b); c)	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
Allegato II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
Allegato II 4.1.2.a); b); c)	elb-deletion-protection-ena bled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzion almente, con conseguente perdita di disponibilità delle applicazioni.
Allegato II 4.1.2.a); b); c)	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
Allegato II 4.1.2.a); b); c)	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	sagemaker-endpoint-configur ation-kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 4.1.2.a); b); c)	secretsmanager-using-cmk	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.
Allegato II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanz a Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.
Allegato II 4.1.2.b)	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'elimina zione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata , potrebbe violare il concetto di funzionalità minima.
Allegato II 4.1.2.b)	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	vpc-network-acl-unused-check	Questa regola garantisc e che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.
Allegato II 4.2.1.a)	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.4	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.
Allegato II 4.2.4	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
Allegato II 4.2.4	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.5	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.3.BAJO.a)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
Allegato II 4.2.6.ALTO.b)	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
Allegato II 4.2.6.ALTO.b)	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.ALTO.b)	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
Allegato II 4.2.6.ALTO.b)	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
Allegato II 4.2.6.BAJO.c)	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
Allegato II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
Allegato II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
Allegato II 4.2.6.BAJO.c)	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Allegato II 4.2.6.BAJO.c)	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	I log di flusso VPC forniscon o record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
Allegato II 4.2.7.BAJO	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.7.BAJO	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
Allegato II 4.2.7.BAJO	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.2.7.BAJO	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
Allegato II 4.3.1	ec2-security-group-attached-to-eni-periodic	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanz a Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.1	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.
Allegato II 4.3.1	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.1	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'elimina zione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata , potrebbe violare il concetto di funzionalità minima.
Allegato II 4.3.1	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.1	vpc-network-acl-unused-check	Questa regola garantisc e che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.
Allegato II 4.1.2.b)	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
Allegato II 4.1.2.b)	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
Allegato II 4.1.2.b)	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
Allegato II 4.1.2.b)	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicam ente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
Allegato II 4.1.2.b)	ebs-snapshot-public-restora ble-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
Allegato II 4.1.2.b)	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.
Allegato II 4.1.2.b)	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
Allegato II 4.1.2.b)	lambda-function-public-acce ss-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
Allegato II 4.1.2.b)	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
Allegato II 4.1.2.b)	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.
Allegato II 4.1.2.b)	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Allegato II 4.1.2.b)	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Allegato II 4.1.2.b)	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
Allegato II 4.1.2.b)	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.1.2.b)	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
Allegato II 4.3.4.c)	vuln-management-plan-exists (Controllo del processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente. Ciò può includere strumenti di gestione delle vulnerabilità, cadenza di scansione ambientale, ruoli e responsabilità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
Allegato II 4.3.7.MEDIA.a)	response-plan-exists-mainta ined (Controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti. Disporre di piani di risposta aggiornat i e formalmente documenta ti può aiutare a garantire che il personale addetto all'intervento comprenda ruoli, responsabilità e processi da seguire durante un incidente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
Allegato II 4.3.8.BAJO	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
Allegato II 4.3.8.BAJO	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
Allegato II 4.3.8.BAJO	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
Allegato II 4.3.8.BAJO	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Allegato II 4.3.8.BAJO	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.BAJO	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
Allegato II 4.3.8.MEDIO	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.MEDIO	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.MEDIO	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
Allegato II 4.3.8.MEDIO	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.MEDIO	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
Allegato II 4.3.8.MEDIO	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
Allegato II 4.3.8.MEDIO	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.MEDIO	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
Allegato II 4.3.8.MEDIO	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Allegato II 4.3.8.MEDIO	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.8.MEDIO	vpc-flow-logs-enabled	I log di flusso VPC forniscon o record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
Allegato II 4.3.10.b)	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i percorsi. AWS CloudTrail

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.3.10.b)	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
Allegato II 4.3.10.d)	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
Allegato II 4.6.2.ALTO	guardduty-non-archived-find ings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighS ev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 4.6.2.BASICA	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
Allegato II 4.6.2.MEDIA	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.2.3	security-awareness-program-exists (Controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.
Allegato II 5.2.4	security-awareness-program-exists (Controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.
Allegato II 5.2.5	security-awareness-program-exists (Controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.2.MEDIO	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 5.4.2.MEDIO	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
Allegato II 5.4.2.MEDIO	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.2.MEDIO	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.4.2.MEDIO	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Allegato II 5.4.2.MEDIO	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Allegato II 5.4.2.MEDIO	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.4.2.MEDIO	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5,4.3.BAJO.a)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
Allegato II 5.4.3.MEDIO	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 5.4.3.MEDIO	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.3.MEDIO	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.4.3.MEDIO	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittogra fate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 5.4.3.MEDIO	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentir e ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.3.MEDIO	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
Allegato II 5.4.3.MEDIO	opensearch-logs-to-cloudwat ch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Allegato II 5.4.3.MEDIO	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.4.3.MEDIO	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.6.1.c)	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.6.1.c)	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub
Allegato II 5.7.3	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 5.7.3	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 5.7.3	s3-default-encryption-kms	Assicurati che la crittogra fia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittogra fia a riposo per proteggere tali dati.
Allegato II 5.7.3	sagemaker-notebook-instance -kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 5.7.3	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentir e ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Allegato II 5.7.3	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
Allegato II 5.7.3	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
Allegato II 5.7.3	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
Allegato II 5.7.3	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
Allegato II 5.7.3	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
Allegato II 5.7.3	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.
Allegato II 5.7.3	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Allegato II 5.7.3	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
Allegato II 5.7.3	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 5.7.3	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.
Allegato II 5.7.4	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.7.4	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
Allegato II 5.8.2	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.2	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
Allegato II 5.8.3.MEDIO.b)	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.3.MEDIO.b)	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
Allegato II 5.8.3.MEDIO.b)	elb-cross-zone-load-balanci ng-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalen ti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.3.MEDIO.b)	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
Allegato II 5.8.3.MEDIO.b)	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.3.MEDIO.b)	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.3.MEDIO.b)	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
Allegato II 5.8.3.MEDIO.b)	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.
Art. 14.4	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 16	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.
Art. 16	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
Art. 16	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 20.2	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
Art. 20.2	vuln-management-plan-exists (Controllo del processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente. Ciò può includere strumenti di gestione delle vulnerabilità, cadenza di scansione ambientale, ruoli e responsabilità.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
Art. 21.1	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Art. 21.1	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.
Art. 21.1	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
Art. 21.1	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
Art. 21.1	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Art. 21.1	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
Art. 21.1	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Art. 21.1	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
Art. 21.1	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
Art. 21.1	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
Art. 21.1	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
Art. 21.1	elb-deletion-protection-ena bled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzion almente, con conseguente perdita di disponibilità delle applicazioni.
Art. 21.1	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
Art. 21.1	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Art. 21.1	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Art. 21.1	sagemaker-endpoint-configur ation-kms-key-configured	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
Art. 21.1	secretsmanager-using-cmk	Per proteggere i dati archiviat i, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 21.1	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.
Art. 22	autoscaling-launch-config-p ublic-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicam ente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
Art. 22	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
Art. 22	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicam ente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
Art. 22	ebs-snapshot-public-restora ble-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
Art. 22	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.
Art. 22	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
Art. 22	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
Art. 22	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
Art. 22	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.
Art. 22	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Art. 22	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Art. 22	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
Art. 22	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di configurazione	Linea guida
Art. 22	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
Art. 23	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
Art. 23	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
Art. 23	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
Art. 23	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
Art. 23	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Art. 23	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 23	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
Art. 24.2	response-plan-exists-maintained (Controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti. Disporre di piani di risposta aggiornati e formalmente documentati può aiutare a garantire che il personale addetto all'intervento comprenda ruoli, responsabilità e processi da seguire durante un incidente.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 24.1	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
Art. 25	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
Art. 25	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
Art. 25	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
Art. 25	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
Art. 25	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	AWS Regola di configurazione	Linea guida
Art. 25	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
Art. 25	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for Esquema Nacional de Seguridad (ENS) High.

Best practice operative per FDA Titolo 21 CFR Parte 11

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il Titolo 21 del Codice dei Regolamenti Federali (CFR) Parte 11 e le regole di AWS Config gestite. Ogni AWS Config regola si applica a una AWS risorsa specifica e si riferisce a uno o più controlli del CFR Parte 11 del Titolo 21 della FDA. Un controllo FDA Titolo 21 CFR Parte 11 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.1	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	includere quanto segue:		
11.1	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue:	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.1	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue:	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.1	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue:	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.1	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue:	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.1	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue:	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.1	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue:	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.1	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue:	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.1	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue:	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.1	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue:	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.1	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue:	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			requisiti dell'orga nizzazione.
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accurat ezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	backup-recovery-po int-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accurat ezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accurat ezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accurat ezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accurat ezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accurat ezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accurat ezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accurat ezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accurat ezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accurat ezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			e le operazioni del database non appena il failover è completato.
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accurat ezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(a)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (a) convalida dei sistemi per garantire l'accuratezza, l'affidabilità, la coerenza delle prestazioni previste e la capacità di individuare record non validi o alterati.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (c) protezion e dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (c) protezione dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (c) protezione dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	ecr-private-lifecycle-policy-configured	Le policy sul ciclo di vita di Amazon Elastic Container Repository (ECR) consentono di specificare la gestione del ciclo di vita delle immagini in un repository. Ciò consente di automatizzare la pulizia delle immagini inutilizzate, come quelle in scadenza in base all'età o al conteggio.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (c) protezione dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (c) protezion e dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (c) protezion e dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (c) protezione dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (c) protezion e dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (c) protezione dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (c) protezion e dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (c) protezione dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (c) protezion e dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (c) protezione dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (c) protezione dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (c) protezion e dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazion i che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (c) protezion e dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	sagemaker-endpoint -configuration-kms- key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (c) protezion e dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	sagemaker-notebook -instance-kms-key- configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11,10(c)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (c) protezione dei record per consentirne l'accurato e pronto recupero per tutto il periodo della loro conservazione.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizza tiva. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	elasticsearch-encr ypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			e altre informazioni amministrative su ogni principale.
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			riflettere le policy dell'organizzazione.
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	root-account-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richieden do l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	s3-bucket-public-w rite-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (d) limitazione dell'accesso al sistema alle persone autorizzate.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(d)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (d) limitazio ne dell'accesso al sistema alle persone autorizzate.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrasse gnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modifican o o eliminano i record elettronici.	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizza tiva. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrassegnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modificano o eliminano i record elettronici.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrasse gnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modifican o o eliminano i record elettronici.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrasse gnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modifican o o eliminano i record elettronici.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrasse gnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modifican o o eliminano i record elettronici.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrassegnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modificano o eliminano i record elettronici.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrasse gnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modifican o o eliminano i record elettronici.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrassegnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modificano o eliminano i record elettronici.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrassegnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modificano o eliminano i record elettronici.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrasse gnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modifican o o eliminano i record elettronici.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrassegnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modificano o eliminano i record elettronici.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrassegnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modificano o eliminano i record elettronici.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrasse gnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modifican o o eliminano i record elettronici.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrassegnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modificano o eliminano i record elettronici.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrasse gnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modifican o o eliminano i record elettronici.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrassegnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modificano o eliminano i record elettronici.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrasse gnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modifican o o eliminano i record elettronici.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrasse gnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modifican o o eliminano i record elettronici.	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrassegnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modificano o eliminano i record elettronici.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrassegnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modificano o eliminano i record elettronici.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integri tà e, se necessari o, la riservatezza e ad assicurare che il firmatario non possa prontamen te rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrasse gnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modifican o o eliminano i record elettronici.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(e)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (e) l'uso di audit trail sicure, generate dal computer e contrassegnate da una data e un'ora per registrare in modo indipendente la data e l'ora degli inserimenti e delle azioni dell'operatore che creano, modificano o eliminano i record elettronici.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	Le modifiche ai record non devono oscurare le informazioni registrate in precedenza. Tale documentazione di audit trail deve essere conservata per un periodo di tempo pari almeno a quello richiesto per i record elettronici in questione e deve essere disponibile per la revisione e la copia da parte dell'agenzia.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizza tiva. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	lambda-function-pu blic-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	root-account-hardw are-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richieden do l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	root-account-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richieden do l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'autorità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettronicamente un record, accedere all'operazione o al dispositivo di input o output del sistema informatico, modificare un record o	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(g)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (g) l'uso di verifiche dell'auto rità per garantire che solo le persone autorizzate possano utilizzare il sistema, firmare elettroni camente un record, accedere all'opera zione o al dispositivo di input o output del sistema informatico, modificare un record o	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	eseguire l'operazione in questione.		
11.10(h)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli includeranno quanto segue: (h) Controlli sull'uso del dispositivo (ad esempio, il terminale) per determinare, se del caso, la validità della fonte di immissione dei dati o delle istruzioni operative.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(h)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (h) Controlli sull'uso del dispositivo (ad esempio, il terminale) per determinare, se del caso, la validità della fonte di immission e dei dati o delle istruzioni operative.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(h)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (h) Controllo dell'uso del dispositi vo (ad esempio, del terminale) per determinare, se del caso, la validità della fonte di immission e dei dati o delle istruzioni operative.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(i)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (i) la verifica che le persone che sviluppano, mantengono o utilizzano sistemi di record elettronici/firme elettroniche abbiano le competenze, la formazione e l'esperie nza necessarie per svolgere le attività loro assegnate.	security-awareness -program-exists (controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organiz zazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documentazione per il funzionamento e la manutenzione del sistema. (2) Procedure di controllo delle revisioni e	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documentazione per il funzionamento e la manutenzione del sistema. (2) Procedure di controllo delle revisioni e	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	s3-bucket-public-w rite-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	ssm-document-not-p ublic	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservar e o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenti cità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico . Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documenta zione per il funzionam ento e la manutenzi one del sistema. (2) Procedure di controllo delle revisioni e	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.10(k)	Le persone che utilizzano sistemi chiusi per creare, modificare, conservare o trasmettere record elettronici devono impiegare procedure e controlli volti a garantirne l'autenticità, l'integrità e, se necessario, la riservatezza e ad assicurare che il firmatario non possa prontamente rifiutare il record firmato in quanto non autentico. Tali procedure e controlli devono includere quanto segue: (k) uso di controlli appropriati sulla documentazione del sistema, tra cui: (1) controlli adeguati sulla distribuzione, l'accesso e l'uso della documentazione per il funzionamento e la manutenzione del sistema. (2) Procedure di controllo delle revisioni e	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	delle modifiche per mantenere un a audit trail che documenti lo sviluppo e la modifica in sequenza temporale della documentazione dei sistemi.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	(a) Le firme elettroni che non basate sulla biometria devono: (1) utilizzare almeno due componenti di identificazione distinti, quali un codice di identificazione e una password. (i) Quando una persona esegue una serie di firme durante un singolo periodo continuo di accesso controllato al sistema, la prima firma deve essere eseguita utilizzan do tutti i component i della firma elettroni ca; le firme successiv e devono essere eseguite utilizzando almeno un component e della firma elettroni ca eseguibile solo dalla persona e progettato per essere utilizzato solo da questa. (ii) Quando una persona esegue una o più firme non realizzate durante un singolo periodo	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizza tiva. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	continuo di accesso controllato al sistema, ogni firma deve essere eseguita utilizzando tutti i componenti di firma elettronica. (2) Essere utilizzate solo dai loro veri proprietari; e (3) essere amministrate ed eseguite in modo da garantire che il tentativo di utilizzo della firma elettroni ca di una persona da parte di chiunque non sia il suo vero proprietario richieda la collaborazione di due o più persone.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	(a) Le firme elettroni che non basate sulla biometria devono: (1) utilizzare almeno due componenti di identificazione distinti, quali un codice di identificazione e una password. (i) Quando una persona esegue una serie di firme durante un singolo periodo continuo di accesso controllato al sistema, la prima firma deve essere eseguita utilizzan do tutti i component i della firma elettroni ca; le firme successiv e devono essere eseguite utilizzando almeno un component e della firma elettroni ca eseguibile solo dalla persona e progettato per essere utilizzato solo da questa. (ii) Quando una persona esegue una o più firme non realizzate durante un singolo periodo	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	continuo di accesso controllato al sistema, ogni firma deve essere eseguita utilizzando tutti i componenti di firma elettronica. (2) Essere utilizzate solo dai loro veri proprietari; e (3) essere amministrate ed eseguite in modo da garantire che il tentativo di utilizzo della firma elettronica di una persona da parte di chiunque non sia il suo vero proprietario richieda la collaborazione di due o più persone.		Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	(a) Le firme elettroni che non basate sulla biometria devono: (1) utilizzare almeno due componenti di identificazione distinti, quali un codice di identificazione e una password. (i) Quando una persona esegue una serie di firme durante un singolo periodo continuo di accesso controllato al sistema, la prima firma deve essere eseguita utilizzan do tutti i component i della firma elettroni ca; le firme successiv e devono essere eseguite utilizzando almeno un component e della firma elettroni ca eseguibile solo dalla persona e progettato per essere utilizzato solo da questa. (ii) Quando una persona esegue una o più firme non realizzate durante un singolo periodo	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	continuo di accesso controllato al sistema, ogni firma deve essere eseguita utilizzando tutti i componenti di firma elettronica. (2) Essere utilizzate solo dai loro veri proprietari; e (3) essere amministrate ed eseguite in modo da garantire che il tentativo di utilizzo della firma elettroni ca di una persona da parte di chiunque non sia il suo vero proprietario richieda la collaborazione di due o più persone.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	(a) Le firme elettroni che non basate sulla biometria devono: (1) utilizzare almeno due componenti di identificazione distinti, quali un codice di identificazione e una password. (i) Quando una persona esegue una serie di firme durante un singolo periodo continuo di accesso controllato al sistema, la prima firma deve essere eseguita utilizzan do tutti i component i della firma elettroni ca; le firme successiv e devono essere eseguite utilizzando almeno un component e della firma elettroni ca eseguibile solo dalla persona e progettato per essere utilizzato solo da questa. (ii) Quando una persona esegue una o più firme non realizzate durante un singolo periodo	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	continuo di accesso controllato al sistema, ogni firma deve essere eseguita utilizzando tutti i componenti di firma elettronica. (2) Essere utilizzate solo dai loro veri proprietari; e (3) essere amministrate ed eseguite in modo da garantire che il tentativo di utilizzo della firma elettroni ca di una persona da parte di chiunque non sia il suo vero proprietario richieda la collaborazione di due o più persone.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	(a) Le firme elettroni che non basate sulla biometria devono: (1) utilizzare almeno due componenti di identificazione distinti, quali un codice di identificazione e una password. (i) Quando una persona esegue una serie di firme durante un singolo periodo continuo di accesso controllato al sistema, la prima firma deve essere eseguita utilizzan do tutti i component i della firma elettroni ca; le firme successiv e devono essere eseguite utilizzando almeno un component e della firma elettroni ca eseguibile solo dalla persona e progettato per essere utilizzato solo da questa. (ii) Quando una persona esegue una o più firme non realizzate durante un singolo periodo	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	continuo di accesso controllato al sistema, ogni firma deve essere eseguita utilizzando tutti i componenti di firma elettronica. (2) Essere utilizzate solo dai loro veri proprietari; e (3) essere amministrate ed eseguite in modo da garantire che il tentativo di utilizzo della firma elettroni ca di una persona da parte di chiunque non sia il suo vero proprietario richieda la collaborazione di due o più persone.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	(a) Le firme elettroni che non basate sulla biometria devono: (1) utilizzare almeno due componenti di identificazione distinti, quali un codice di identificazione e una password. (i) Quando una persona esegue una serie di firme durante un singolo periodo continuo di accesso controllato al sistema, la prima firma deve essere eseguita utilizzan do tutti i component i della firma elettroni ca; le firme successiv e devono essere eseguite utilizzando almeno un component e della firma elettroni ca eseguibile solo dalla persona e progettato per essere utilizzato solo da questa. (ii) Quando una persona esegue una o più firme non realizzate durante un singolo periodo	root-account-hardw are-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richieden do l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	continuo di accesso controllato al sistema, ogni firma deve essere eseguita utilizzando tutti i componenti di firma elettronica. (2) Essere utilizzate solo dai loro veri proprietari; e (3) essere amministrate ed eseguite in modo da garantire che il tentativo di utilizzo della firma elettroni ca di una persona da parte di chiunque non sia il suo vero proprietario richieda la collaborazione di due o più persone.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.2	(a) Le firme elettroni che non basate sulla biometria devono: (1) utilizzare almeno due componenti di identificazione distinti, quali un codice di identificazione e una password. (i) Quando una persona esegue una serie di firme durante un singolo periodo continuo di accesso controllato al sistema, la prima firma deve essere eseguita utilizzan do tutti i component i della firma elettroni ca; le firme successiv e devono essere eseguite utilizzando almeno un component e della firma elettroni ca eseguibile solo dalla persona e progettato per essere utilizzato solo da questa. (ii) Quando una persona esegue una o più firme non realizzate durante un singolo periodo	root-account-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richieden do l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
	continuo di accesso controllato al sistema, ogni firma deve essere eseguita utilizzando tutti i componenti di firma elettronica. (2) Essere utilizzate solo dai loro veri proprietari; e (3) essere amministrate ed eseguite in modo da garantire che il tentativo di utilizzo della firma elettroni ca di una persona da parte di chiunque non sia il suo vero proprietario richieda la collaborazione di due o più persone.		

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservare o trasmettere documenti elettronici devono impiegare procedure e controlli volti a garantire l'autenticità, l'integrità e, se necessario, la riservatezza dei documenti elettronici dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntive quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservare o trasmettere documenti elettronici devono impiegare procedure e controlli volti a garantire l'autenticità, l'integrità e, se necessario, la riservatezza dei documenti elettronici dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntive quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservare o trasmettere documenti elettronici devono impiegare procedure e controlli volti a garantire l'autenticità, l'integrità e, se necessario, la riservatezza dei documenti elettronici dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntive quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	codebuild-project-s3-logs-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per AWS CodeBuild i log archiviati in Amazon S3.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservare o trasmettere documenti elettronici devono impiegare procedure e controlli volti a garantire l'autenticità, l'integrità e, se necessario, la riservatezza dei documenti elettronici dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntive quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	elasticsearch-encr ypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	elasticsearch-encr ypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservare o trasmettere documenti elettronici devono impiegare procedure e controlli volti a garantire l'autenticità, l'integrità e, se necessario, la riservatezza dei documenti elettronici dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntive quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservare o trasmettere documenti elettronici devono impiegare procedure e controlli volti a garantire l'autenticità, l'integrità e, se necessario, la riservatezza dei documenti elettronici dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntive quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	opensearch-encrypt ed-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservare o trasmettere documenti elettronici devono impiegare procedure e controlli volti a garantire l'autenticità, l'integrità e, se necessario, la riservatezza dei documenti elettronici dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntive quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservare o trasmettere documenti elettronici devono impiegare procedure e controlli volti a garantire l'autenticità, l'integrità e, se necessario, la riservatezza dei documenti elettronici dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntive quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservare o trasmettere documenti elettronici devono impiegare procedure e controlli volti a garantire l'autenticità, l'integrità e, se necessario, la riservatezza dei documenti elettronici dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntive quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservare o trasmettere documenti elettronici devono impiegare procedure e controlli volti a garantire l'autenticità, l'integrità e, se necessario, la riservatezza dei documenti elettronici dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntive quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservare o trasmettere documenti elettronici devono impiegare procedure e controlli volti a garantire l'autenticità, l'integrità e, se necessario, la riservatezza dei documenti elettronici dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntive quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	sagemaker-endpoint -configuration-kms- key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	sagemaker-notebook -instance-kms-key- configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservare o trasmettere documenti elettronici devono impiegare procedure e controlli volti a garantire l'autenticità, l'integrità e, se necessario, la riservatezza dei documenti elettronici dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntive quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.3	Le persone che utilizzano sistemi aperti per creare, modificare, conservar e o trasmettere documenti elettroni ci devono impiegare procedure e controlli volti a garantire l'autenticità, l'integri tà e, se necessario, la riservatezza dei documenti elettroni ci dal momento della loro creazione al momento della loro ricezione. Tali procedure e controlli includeranno quelli identificati in 11.10, come appropriato, e misure aggiuntiv e quali la crittografia dei documenti e l'uso di standard di firma digitale appropriati per garantire, come necessario in base alle circostanze, l'autenticità, l'integrità e la riservatezza dei record.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.300(b)	Le persone che utilizzano firme elettroniche basate sull'uso di codici di identificazione in combinazione con password devono adottare controlli per garantirne la sicurezza e l'integrità. Tali controlli includera nno: (b) Garantire che l'emissione di codici di identific azione e password venga periodica mente verificata, richiamata o rivista (ad esempio, per coprire eventi come l'invecchiamento delle password).	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizza tiva. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.300(b)	Le persone che utilizzano firme elettroniche basate sull'uso di codici di identificazione in combinazione con password devono adottare controlli per garantirne la sicurezza e l'integrità. Tali controlli includera nno: (b) Garantire che l'emissione di codici di identific azione e password venga periodica mente verificata, richiamata o rivista (ad esempio, per coprire eventi come l'invecchiamento delle password).	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.300(b)	Le persone che utilizzano firme elettroniche basate sull'uso di codici di identificazione in combinazione con password devono adottare controlli per garantirne la sicurezza e l'integrità. Tali controlli includeranno: (b) Garantire che l'emissione di codici di identificazione e password venga periodicamente verificata, richiamata o rivista (ad esempio, per coprire eventi come l'invecchiamento della password).	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.300(b)	Le persone che utilizzano firme elettroniche basate sull'uso di codici di identificazione in combinazione con password devono adottare controlli per garantirne la sicurezza e l'integrità. Tali controlli includeranno: (b) Garantire che l'emissione di codici di identificazione e password venga periodicamente verificata, richiamata o rivista (ad esempio, per coprire eventi come l'invecchiamento delle password).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.300(b)	Le persone che utilizzano firme elettroniche basate sull'uso di codici di identificazione in combinazione con password devono adottare controlli per garantirne la sicurezza e l'integrità. Tali controlli includera nno: (b) Garantire che l'emissione di codici di identific azione e password venga periodica mente verificata, richiamata o rivista (ad esempio, per coprire eventi come l'invecchiamento delle password).	secretsmanager-rot ation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianifica zione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromis sione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.300(b)	Le persone che utilizzano firme elettroniche basate sull'uso di codici di identificazione in combinazione con password devono adottare controlli per garantirne la sicurezza e l'integrità. Tali controlli devono includere: (b) Garantire che l'emissione di codici di identificazione e password venga periodicamente verificata, richiamata o rivista (ad esempio, per coprire eventi come l'invecchiamento delle password).	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.300(d)	Le persone che utilizzano firme elettroniche basate sull'uso di codici di identificazione in combinazione con password devono adottare controlli per garantirne la sicurezza e l'integri tà. Tali controlli comprendono: (d) impiego di misure di salvaguardia delle transazioni per prevenire l'uso non autorizzato di password e/o codici di identificazione e per rilevare e segnalare in modo immediato e urgente qualsiasi tentativo di uso non autorizzato all'unità di sicurezza del sistema e, se necessario, alla direzione dell'orga nizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.300(d)	Le persone che utilizzano firme elettroniche basate sull'uso di codici di identificazione in combinazione con password devono adottare controlli per garantirne la sicurezza e l'integri tà. Tali controlli comprendono: (d) impiego di misure di salvaguardia delle transazioni per prevenire l'uso non autorizzato di password e/o codici di identificazione e per rilevare e segnalare in modo immediato e urgente qualsiasi tentativo di uso non autorizzato all'unità di sicurezza del sistema e, se necessario, alla direzione dell'orga nizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.300(d)	Le persone che utilizzano firme elettroniche basate sull'uso di codici di identificazione in combinazione con password devono adottare controlli per garantirne la sicurezza e l'integri tà. Tali controlli comprendono: (d) impiego di misure di salvaguardia delle transazioni per prevenire l'uso non autorizzato di password e/o codici di identificazione e per rilevare e segnalare in modo immediato e urgente qualsiasi tentativo di uso non autorizzato all'unità di sicurezza del sistema e, se necessario, alla direzione dell'orga nizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di configurazione	Linea guida
11.300(d)	Le persone che utilizzano firme elettroniche basate sull'uso di codici di identificazione in combinazione con password devono adottare controlli per garantirne la sicurezza e l'integri tà. Tali controlli comprendono: (d) impiego di misure di salvaguardia delle transazioni per prevenire l'uso non autorizzato di password e/o codici di identificazione e per rilevare e segnalare in modo immediato e urgente qualsiasi tentativo di uso non autorizzato all'unità di sicurezza del sistema e, se necessario, alla direzione dell'orga nizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

Modello

Il modello è disponibile su GitHub: Operational Best Practices for FDA Title 21 CFR Part 11.

Best practice operative per FedRAMP (Low)

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra i controlli Low Baseline del Federal Risk and Authorization Management Program (FedRAMP) e le regole di Config gestite. AWS Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli FedRAMP. Un controllo FedRAMP può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.
AC-2	GESTIONE DELL'ACCOUNT	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC-2	GESTIONE DELL'ACCOUNT	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizza tiva. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AC-2	GESTIONE DELL'ACCOUNT	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	GESTIONE DELL'ACCOUNT	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
AC-3	APPLICAZIONE DEGLI ACCESSI	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
AC-3	APPLICAZIONE DEGLI ACCESSI	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC-3	APPLICAZIONE DEGLI ACCESSI	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-3	APPLICAZIONE DEGLI ACCESSI	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC-3	APPLICAZIONE DEGLI ACCESSI	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-3	APPLICAZIONE DEGLI ACCESSI	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC-3	APPLICAZIONE DEGLI ACCESSI	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-3	APPLICAZIONE DEGLI ACCESSI	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	APPLICAZIONE DEGLI ACCESSI	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
AC-17	ACCESSO REMOTO	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
AC-17	ACCESSO REMOTO	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-17	ACCESSO REMOTO	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-17	ACCESSO REMOTO	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-17	ACCESSO REMOTO	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
AC-17	ACCESSO REMOTO	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC-17	ACCESSO REMOTO	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-17	ACCESSO REMOTO	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC-17	ACCESSO REMOTO	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17	ACCESSO REMOTO	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	EVENTI DI AUDIT	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	EVENTI DI AUDIT	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	EVENTI DI AUDIT	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	EVENTI DI AUDIT	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AU-2	EVENTI DI AUDIT	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	EVENTI DI AUDIT	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU-2	EVENTI DI AUDIT	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	EVENTI DI AUDIT	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU-2	EVENTI DI AUDIT	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	EVENTI DI AUDIT	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	EVENTI DI AUDIT	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	EVENTI DI AUDIT	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
AU-3	CONTENUTO DEI RECORD DI AUDIT	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	CONTENUTO DEI RECORD DI AUDIT	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	CONTENUTO DEI RECORD DI AUDIT	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	CONTENUTO DEI RECORD DI AUDIT	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AU-3	CONTENUTO DEI RECORD DI AUDIT	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	CONTENUTO DEI RECORD DI AUDIT	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU-3	CONTENUTO DEI RECORD DI AUDIT	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	CONTENUTO DEI RECORD DI AUDIT	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU-3	CONTENUTO DEI RECORD DI AUDIT	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	CONTENUTO DEI RECORD DI AUDIT	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	CONTENUTO DEI RECORD DI AUDIT	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	CONTENUTO DEI RECORD DI AUDIT	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6	REVISIONE, ANALISI E REPORTING DEGLI AUDIT	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
AU-9	PROTEZIONE DELLE INFORMAZIONI DI AUDIT	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9	PROTEZIONE DELLE INFORMAZIONI DI AUDIT	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9	PROTEZIONE DELLE INFORMAZIONI DI AUDIT	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9	PROTEZIONE DELLE INFORMAZIONI DI AUDIT	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
AU-9	PROTEZIONE DELLE INFORMAZIONI DI AUDIT	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-11	CONSERVAZIONE DEI RECORD DI AUDIT	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.
AU-12	GENERAZIONE DI AUDIT	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	GENERAZIONE DI AUDIT	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	GENERAZIONE DI AUDIT	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	GENERAZIONE DI AUDIT	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AU-12	GENERAZIONE DI AUDIT	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	GENERAZIONE DI AUDIT	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU-12	GENERAZIONE DI AUDIT	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	GENERAZIONE DI AUDIT	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU-12	GENERAZIONE DI AUDIT	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	GENERAZIONE DI AUDIT	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	GENERAZIONE DI AUDIT	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	GENERAZIONE DI AUDIT	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
CA-7	MONITORAGGIO CONTINUO	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	MONITORAGGIO CONTINUO	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	MONITORAGGIO CONTINUO	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	MONITORAGGIO CONTINUO	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	MONITORAGGIO CONTINUO	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	MONITORAGGIO CONTINUO	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	MONITORAGGIO CONTINUO	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	MONITORAGGIO CONTINUO	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
CA-7	MONITORAGGIO CONTINUO	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	MONITORAGGIO CONTINUO	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	MONITORAGGIO CONTINUO	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CA-7	MONITORAGGIO CONTINUO	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.
CA-7	MONITORAGGIO CONTINUO	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	MONITORAGGIO CONTINUO	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
CM-2	CONFIGURAZIONE DI BASE	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM-2	CONFIGURAZIONE DI BASE	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM-2	CONFIGURAZIONE DI BASE	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
CM-2	CONFIGURAZIONE DI BASE	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
CM-2	CONFIGURAZIONE DI BASE	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CM-2	CONFIGURAZIONE DI BASE	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
CM-2	CONFIGURAZIONE DI BASE	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	CONFIGURAZIONE DI BASE	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CM-2	CONFIGURAZIONE DI BASE	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-7	FUNZIONALITÀ MINIMA	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.
CM-7	FUNZIONALITÀ MINIMA	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-7	FUNZIONALITÀ MINIMA	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8	INVENTARIO DEI COMPONENTI DEL SISTEMA INFORMATIVO	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8	INVENTARIO DEI COMPONENTI DEL SISTEMA INFORMATIVO	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8	INVENTARIO DEI COMPONENTI DEL SISTEMA INFORMATIVO	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8	INVENTARIO DEI COMPONENTI DEL SISTEMA INFORMATIVO	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	BACKUP DEL SISTEMA INFORMATIVO	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	BACKUP DEL SISTEMA INFORMATIVO	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CP-9	BACKUP DEL SISTEMA INFORMATIVO	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	BACKUP DEL SISTEMA INFORMATIVO	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	BACKUP DEL SISTEMA INFORMATIVO	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	BACKUP DEL SISTEMA INFORMATIVO	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	BACKUP DEL SISTEMA INFORMATIVO	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	BACKUP DEL SISTEMA INFORMATIVO	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	BACKUP DEL SISTEMA INFORMATIVO	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	BACKUP DEL SISTEMA INFORMATIVO	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
CP-9	BACKUP DEL SISTEMA INFORMATIVO	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	BACKUP DEL SISTEMA INFORMATIVO	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	BACKUP DEL SISTEMA INFORMATIVO	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	BACKUP DEL SISTEMA INFORMATIVO	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	RIPRISTINO E RICOSTITUZIONE DEL SISTEMA INFORMATIVO	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2	IDENTIFICAZIONE E AUTENTICAZIONE (UTENTI DELL'ORGANIZZAZIONE)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2	IDENTIFICAZIONE E AUTENTICAZIONE (UTENTI DELL'ORGANIZZAZIONE)	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2	IDENTIFICAZIONE E AUTENTICAZIONE (UTENTI DELL'ORGANIZZAZIONE)	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2	IDENTIFICAZIONE E AUTENTICAZIONE (UTENTI DELL'ORGANIZZAZIONE)	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2	IDENTIFICAZIONE E AUTENTICAZIONE (UTENTI DELL'ORGANIZZAZIONE)	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2	IDENTIFICAZIONE E AUTENTICAZIONE (UTENTI DELL'ORGANIZZAZIONE)	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-5	GESTIONE DEGLI AUTENTICATORI	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-5	GESTIONE DEGLI AUTENTICATORI	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundatio

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			nal Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-4	GESTIONE DEGLI INCIDENTI	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-4	GESTIONE DEGLI INCIDENTI	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-4	GESTIONE DEGLI INCIDENTI	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-4	GESTIONE DEGLI INCIDENTI	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-4	GESTIONE DEGLI INCIDENTI	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-6	REPORT DEGLI INCIDENTI	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-6	REPORT DEGLI INCIDENTI	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-6	REPORT DEGLI INCIDENTI	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-7	ASSISTENZA PER LA RISPOSTA AGLI INCIDENTI	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-7	ASSISTENZA PER LA RISPOSTA AGLI INCIDENTI	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-7	ASSISTENZA PER LA RISPOSTA AGLI INCIDENTI	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA-5	SCANSIONE DELLE VULNERABILITÀ	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA-5	SCANSIONE DELLE VULNERABILITÀ	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA-5	SCANSIONE DELLE VULNERABILITÀ	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-3	CICLO DI VITA DI SVILUPPO DEL SISTEMA	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-3	CICLO DI VITA DI SVILUPPO DEL SISTEMA	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-3	CICLO DI VITA DI SVILUPPO DEL SISTEMA	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	PROTEZIONE DAL RIFIUTO DEL SERVIZIO	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
SC-7	PROTEZIONE DEI CONFINI	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC-7	PROTEZIONE DEI CONFINI	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
SC-7	PROTEZIONE DEI CONFINI	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-7	PROTEZIONE DEI CONFINI	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
SC-7	PROTEZIONE DEI CONFINI	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC-7	PROTEZIONE DEI CONFINI	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-7	PROTEZIONE DEI CONFINI	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	PROTEZIONE DEI CONFINI	waf-regional-webacl-not-empty	Un ACL Web collegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.
SC-12	CREAZIONE E GESTIONE DELLE CHIAVI CRITTOGRAFICHE	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12	CREAZIONE E GESTIONE DELLE CHIAVI CRITTOGRAFICHE	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12	CREAZIONE E GESTIONE DELLE CHIAVI CRITTOGRAFICHE	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	PROTEZIONE CRITTOGRAFICA	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel servizio di gestione delle AWS chiavi (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	PROTEZIONE CRITTOGRAFICA	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
SC-13	PROTEZIONE CRITTOGRAFICA	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	PROTEZIONE CRITTOGRAFICA	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	PROTEZIONE CRITTOGRAFICA	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
SC-13	PROTEZIONE CRITTOGRAFICA	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2	CORREZIONE DEI DIFETTI	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2	CORREZIONE DEI DIFETTI	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2	CORREZIONE DEI DIFETTI	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2	CORREZIONE DEI DIFETTI	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3	CORREZIONE DEI DIFETTI	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3	CORREZIONE DEI DIFETTI	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub
SI-3	CORREZIONE DEI DIFETTI	ecs-task-definition-memory-hard-limit	La limitazione della memoria massima disponibile per i container Amazon Elastic Container Service (ECS) garantisce che l'utilizz o delle risorse non possa essere abusato in caso di accesso malevolo ai container.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	MONITORAGGIO DEL SISTEMA INFORMATIVO	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-5	AVVISI, CONSIGLI E DIRETTIVE DI SICUREZZA	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-5	AVVISI, CONSIGLI E DIRETTIVE DI SICUREZZA	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-5	AVVISI, CONSIGLI E DIRETTIVE DI SICUREZZA	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-5	AVVISI, CONSIGLI E DIRETTIVE DI SICUREZZA	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZI ONI	cw-loggroup-retent ion-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzio ne dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruz ione e l'identificazione di eventi potenzial mente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	GESTIONE E CONSERVAZIONE DELLE INFORMAZIONI	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-16	PROTEZIONE DELLA MEMORIA	ecs-task-definition-memory-hard-limit	La limitazione della memoria massima disponibile per i container Amazon Elastic Container Service (ECS) garantisce che l'utilizzo delle risorse non possa essere abusato in caso di accesso malevolo ai container.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for FedRAMP (Low).

Best practice operative per FedRAMP (Moderato)

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il Federal Risk and Authorization Management Program (FedRAMP) e le regole di Config gestite. AWS Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli FedRAMP. Un controllo FedRAMP può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo Conformance Pack è stato convalidato da AWS Security Assurance Services LLC (AWS SAS), che è un team di Payment Card Industry Qualified Security Assessors (QSA), HITRUST Certified Common Security Framework Practitioners (ccSFP) e professionisti della conformità

certificati per fornire linee guida e valutazioni per vari framework di settore. AWS I professionisti SAS hanno progettato questo Conformance Pack per consentire al cliente di allinearsi a un sottoinsieme dei controlli FedRAMP.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizza tiva. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanismi automatizzati per supportare la gestione degli account dei sistemi informativi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanismi automatizzati per supportare la gestione degli account dei sistemi informativi.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanismi automatizzati per supportare la gestione degli account dei sistemi informativi.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanismi automatizzati per supportare la gestione degli account dei sistemi informativi.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	L'organizzazione utilizza meccanismi automatizzati per supportare la gestione degli account dei sistemi informativi.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(3)	Il sistema informativo disattiva automaticamente gli account inattivi per gli utenti dopo 90 giorni.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(3)	Il sistema informativo disattiva automaticamente gli account inattivi per gli utenti dopo 90 giorni.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(7)	L'organizzazione: (a) stabilisce e amministra gli utenti privilegiati in conformità a uno schema di accesso basato sui ruoli che organizza l'accesso al sistema informativo e i privilegi consentiti in ruoli; (b) monitora le assegnazioni di ruoli privilegiati; e (c) adotta [Assegnazione: azioni definite dall'organizzazione] quando le assegnazioni di ruoli privilegiati non sono più appropriate. Guida supplementare: i ruoli con privilegi sono ruoli definiti dall'organizzazione assegnati a persone che consentono loro di eseguire determinate funzioni rilevanti per la sicurezza che gli utenti ordinari non sono autorizzati a svolgere. Questi ruoli con privilegi includono, ad esempio, la	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	gestione delle chiavi, la gestione degli account, l'amminis trazione della rete e del sistema, l'amminis trazione dei database e l'amministrazione web.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(7)	L'organizzazione: (a) stabilisce e amministra gli utenti privilegiati in conformità a uno schema di accesso basato sui ruoli che organizza l'accesso al sistema informativo e i privilegi consentiti in ruoli; (b) monitora le assegnazioni di ruoli privilegiati; e (c) adotta [Assegnazione: azioni definite dall'organizzazione] quando le assegnazioni di ruoli privilegiati non sono più appropriate. Guida supplementare: i ruoli con privilegi sono ruoli definiti dall'organizzazione assegnati a persone che consentono loro di eseguire determinate funzioni rilevanti per la sicurezza che gli utenti ordinari non sono autorizzati a svolgere. Questi ruoli con privilegi includono, ad esempio, la	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	gestione delle chiavi, la gestione degli account, l'amminis trazione della rete e del sistema, l'amminis trazione dei database e l'amministrazione web.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(7)	L'organizzazione: (a) stabilisce e amministra gli utenti privilegiati in conformità a uno schema di accesso basato sui ruoli che organizza l'accesso al sistema informativo e i privilegi consentiti in ruoli; (b) monitora le assegnazioni di ruoli privilegiati; e (c) adotta [Assegnazione: azioni definite dall'organizzazione] quando le assegnazioni di ruoli privilegiati non sono più appropriate. Guida supplementare: i ruoli con privilegi sono ruoli definiti dall'organizzazione assegnati a persone che consentono loro di eseguire determinate funzioni rilevanti per la sicurezza che gli utenti ordinari non sono autorizzati a svolgere. Questi ruoli con privilegi includono, ad esempio, la	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	gestione delle chiavi, la gestione degli account, l'amminis trazione della rete e del sistema, l'amminis trazione dei database e l'amministrazione web.		riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(7)	L'organizzazione: (a) stabilisce e amministra gli utenti privilegiati in conformità a uno schema di accesso basato sui ruoli che organizza l'accesso al sistema informativo e i privilegi consentiti in ruoli; (b) monitora le assegnazioni di ruoli privilegiati; e (c) adotta [Assegnazione: azioni definite dall'organizzazione] quando le assegnazioni di ruoli privilegiati non sono più appropriate. Guida supplementare: i ruoli con privilegi sono ruoli definiti dall'organizzazione assegnati a persone che consentono loro di eseguire determinate funzioni rilevanti per la sicurezza che gli utenti ordinari non sono autorizzati a svolgere. Questi ruoli con privilegi includono, ad esempio, la	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	gestione delle chiavi, la gestione degli account, l'amminis trazione della rete e del sistema, l'amminis trazione dei database e l'amministrazione web.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(7)	L'organizzazione: (a) stabilisce e amministra gli utenti privilegiati in conformità a uno schema di accesso basato sui ruoli che organizza l'accesso al sistema informativo e i privilegi consentiti in ruoli; (b) monitora le assegnazioni di ruoli privilegiati; e (c) adotta [Assegnazione: azioni definite dall'organizzazione] quando le assegnazioni di ruoli privilegiati non sono più appropriate. Guida supplementare: i ruoli con privilegi sono ruoli definiti dall'organizzazione assegnati a persone che consentono loro di eseguire determinate funzioni rilevanti per la sicurezza che gli utenti ordinari non sono autorizzati a svolgere. Questi ruoli con privilegi includono, ad esempio, la	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	gestione delle chiavi, la gestione degli account, l'amminis trazione della rete e del sistema, l'amminis trazione dei database e l'amministrazione web.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(7)	L'organizzazione: (a) stabilisce e amministra gli utenti privilegiati in conformità a uno schema di accesso basato sui ruoli che organizza l'accesso al sistema informativo e i privilegi consentiti in ruoli; (b) monitora le assegnazioni di ruoli privilegiati; e (c) adotta [Assegnazione: azioni definite dall'organizzazione] quando le assegnazioni di ruoli privilegiati non sono più appropriate. Guida supplementare: i ruoli con privilegi sono ruoli definiti dall'organizzazione assegnati a persone che consentono loro di eseguire determinate funzioni rilevanti per la sicurezza che gli utenti ordinari non sono autorizzati a svolgere. Questi ruoli con privilegi includono, ad esempio, la	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	gestione delle chiavi, la gestione degli account, l'amminis trazione della rete e del sistema, l'amminis trazione dei database e l'amministrazione web.		
AC-2(12)(a)	L'organizzazione: a. Monitora gli account del sistema informati vo per [Assegnazione: uso atipico definito dall'organizzazione].	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(12)(a)	L'organizzazione: a. Monitora gli account del sistema informativo per [Assegnazione: uso atipico definito dall'organizzazione].	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indiriz zo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformit à degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.
AC-2(j)	L'organizzazione: j. Verifica la conformit à degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformit à degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizza zioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizza zioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
AC-6(10)	Il sistema informativo impedisce agli utenti non privilegiati di eseguire funzioni privilegiate, tra cui la disabilitazione, l'elusione o la modifica delle protezioni/contromisure di sicurezza implementate.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(10)	Il sistema informativo impedisce agli utenti non privilegiati di eseguire funzioni privilegiate, tra cui la disabilitazione, l'elusione o la modifica delle protezioni/contromisure di sicurezza implementate.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(10)	Il sistema informativo impedisce agli utenti non privilegiati di eseguire funzioni privilegiate, tra cui la disabilitazione, l'elusione o la modifica delle protezioni/contromisure di sicurezza implementate.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'inter no del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	dms-replication-not-public	Gestisci l'accesso al cloud assicurando che AWS le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	s3-bucket-public-w rite-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	sagemaker-notebook -no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(2)	Il sistema informativo implementa meccanismi crittografici per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC-17(2)	Il sistema informativo implementa meccanismi crittografici per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto.	acm-certificate-expiration-check	Garantisci che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(2)	Il sistema informativo implementa meccanismi crittografici per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC-17(2)	Il sistema informativo implementa meccanismi crittografici per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(2)	Il sistema informativo implementa meccanismi crittografici per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2(a)(d)	L'organizzazione: a. Verifica che il sistema informativo sia in grado di eseguire l'auditing dei seguenti eventi: eventi di accesso all'account riusciti e non riusciti, eventi di gestione dell'account, accesso agli oggetti, modifica dei criteri, funzioni di privilegio, tracciamento dei processi ed eventi di sistema. Per le applicazioni web: tutte le attività dell'amministratore, i controlli di autenticazione, i controlli di autorizzazione, le eliminazioni di dati, l'accesso ai dati, le modifiche dei dati e le modifiche dei permessi. d. Stabilisce che i seguenti eventi devono essere sottoposti ad audit all'interno del sistema informativo: [sottoinsieme definito dall'organizzazione degli	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	eventi verificabili definiti in AU-2 a da verificare continuam ente per ogni evento identificato].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2(a)(d)	L'organizzazione: a. Verifica che il sistema informati vo sia in grado di eseguire l'auditing dei seguenti eventi: eventi di accesso all'account riusciti e non riusciti, eventi di gestione dell'account, accesso agli oggetti, modifica dei criteri, funzioni di privilegi o, tracciamento dei processi ed eventi di sistema. Per le applicazioni web: tutte le attività dell'ammi nistratore, i controlli di autenticazione, i controlli di autorizza zione, le eliminazioni di dati, l'accesso ai dati, le modifiche dei dati e le modifiche dei permessi. d. Stabilisc e che i seguenti eventi devono essere sottoposti ad audit all'interno del sistema informativo: [sottoins ieme definito dall'orga nizzazione degli	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	eventi verificabili definiti in AU-2 a da verificare continuam ente per ogni evento identificato].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2(a)(d)	L'organizzazione: a. Verifica che il sistema informati vo sia in grado di eseguire l'auditing dei seguenti eventi: eventi di accesso all'account riusciti e non riusciti, eventi di gestione dell'account, accesso agli oggetti, modifica dei criteri, funzioni di privilegi o, tracciamento dei processi ed eventi di sistema. Per le applicazioni web: tutte le attività dell'ammi nistratore, i controlli di autenticazione, i controlli di autorizza zione, le eliminazioni di dati, l'accesso ai dati, le modifiche dei dati e le modifiche dei permessi. d. Stabilisc e che i seguenti eventi devono essere sottoposti ad audit all'interno del sistema informativo: [sottoins ieme definito dall'orga nizzazione degli	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	eventi verificabili definiti in AU-2 a da verificare continuam ente per ogni evento identificato].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2(a)(d)	L'organizzazione: a. Verifica che il sistema informativo sia in grado di eseguire l'auditing dei seguenti eventi: eventi di accesso all'account riusciti e non riusciti, eventi di gestione dell'account, accesso agli oggetti, modifica dei criteri, funzioni di privilegio, tracciamento dei processi ed eventi di sistema. Per le applicazioni web: tutte le attività dell'amministratore, i controlli di autenticazione, i controlli di autorizzazione, le eliminazioni di dati, l'accesso ai dati, le modifiche dei dati e le modifiche dei permessi. d. Stabilisce che i seguenti eventi devono essere sottoposti ad audit all'interno del sistema informativo: [sottoinsieme definito dall'organizzazione degli	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	eventi verificabili definiti in AU-2 a da verificare continuam ente per ogni evento identificato].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2(a)(d)	L'organizzazione: a. Verifica che il sistema informativo sia in grado di eseguire l'auditing dei seguenti eventi: eventi di accesso all'account riusciti e non riusciti, eventi di gestione dell'account, accesso agli oggetti, modifica dei criteri, funzioni di privilegio, tracciamento dei processi ed eventi di sistema. Per le applicazioni web: tutte le attività dell'amministratore, i controlli di autenticazione, i controlli di autorizzazione, le eliminazioni di dati, l'accesso ai dati, le modifiche dei dati e le modifiche dei permessi. d. Stabilisce che i seguenti eventi devono essere sottoposti ad audit all'interno del sistema informativo: [sottoinsieme definito dall'organizzazione degli	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	eventi verificabili definiti in AU-2 a da verificare continuam ente per ogni evento identificato].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2(a)(d)	L'organizzazione: a. Verifica che il sistema informati vo sia in grado di eseguire l'auditing dei seguenti eventi: eventi di accesso all'account riusciti e non riusciti, eventi di gestione dell'account, accesso agli oggetti, modifica dei criteri, funzioni di privilegi o, tracciamento dei processi ed eventi di sistema. Per le applicazioni web: tutte le attività dell'ammi nistratore, i controlli di autenticazione, i controlli di autorizza zione, le eliminazioni di dati, l'accesso ai dati, le modifiche dei dati e le modifiche dei permessi. d. Stabilisc e che i seguenti eventi devono essere sottoposti ad audit all'interno del sistema informativo: [sottoins ieme definito dall'orga nizzazione degli	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	eventi verificabili definiti in AU-2 a da verificare continuam ente per ogni evento identificato].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2(a)(d)	L'organizzazione: a. Verifica che il sistema informati vo sia in grado di eseguire l'auditing dei seguenti eventi: eventi di accesso all'account riusciti e non riusciti, eventi di gestione dell'account, accesso agli oggetti, modifica dei criteri, funzioni di privilegi o, tracciamento dei processi ed eventi di sistema. Per le applicazioni web: tutte le attività dell'ammi nistratore, i controlli di autenticazione, i controlli di autorizza zione, le eliminazioni di dati, l'accesso ai dati, le modifiche dei dati e le modifiche dei permessi. d. Stabilisc e che i seguenti eventi devono essere sottoposti ad audit all'interno del sistema informativo: [sottoins ieme definito dall'orga nizzazione degli	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indiriz zo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	eventi verificabili definiti in AU-2 a da verificare continuam ente per ogni evento identificato].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2(a)(d)	L'organizzazione: a. Verifica che il sistema informativo sia in grado di eseguire l'auditing dei seguenti eventi: eventi di accesso all'account riusciti e non riusciti, eventi di gestione dell'account, accesso agli oggetti, modifica dei criteri, funzioni di privilegio, tracciamento dei processi ed eventi di sistema. Per le applicazioni web: tutte le attività dell'amministratore, i controlli di autenticazione, i controlli di autorizzazione, le eliminazioni di dati, l'accesso ai dati, le modifiche dei dati e le modifiche dei permessi. d. Stabilisce che i seguenti eventi devono essere sottoposti ad audit all'interno del sistema informativo: [sottoinsieme definito dall'organizzazione degli	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	eventi verificabili definiti in AU-2 a da verificare continuam ente per ogni evento identificato].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2(a)(d)	L'organizzazione: a. Verifica che il sistema informativo sia in grado di eseguire l'auditing dei seguenti eventi: eventi di accesso all'account riusciti e non riusciti, eventi di gestione dell'account, accesso agli oggetti, modifica dei criteri, funzioni di privilegio, tracciamento dei processi ed eventi di sistema. Per le applicazioni web: tutte le attività dell'amministratore, i controlli di autenticazione, i controlli di autorizzazione, le eliminazioni di dati, l'accesso ai dati, le modifiche dei dati e le modifiche dei permessi. d. Stabilisce che i seguenti eventi devono essere sottoposti ad audit all'interno del sistema informativo: [sottoinsieme definito dall'organizzazione degli	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	eventi verificabili definiti in AU-2 a da verificare continuam ente per ogni evento identificato].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2(a)(d)	L'organizzazione: a. Verifica che il sistema informativo sia in grado di eseguire l'auditing dei seguenti eventi: eventi di accesso all'account riusciti e non riusciti, eventi di gestione dell'account, accesso agli oggetti, modifica dei criteri, funzioni di privilegio, tracciamento dei processi ed eventi di sistema. Per le applicazioni web: tutte le attività dell'amministratore, i controlli di autenticazione, i controlli di autorizzazione, le eliminazioni di dati, l'accesso ai dati, le modifiche dei dati e le modifiche dei permessi. d. Stabilisce che i seguenti eventi devono essere sottoposti ad audit all'interno del sistema informativo: [sottoinsieme definito dall'organizzazione degli	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	eventi verificabili definiti in AU-2 a da verificare continuam ente per ogni evento identificato].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2(a)(d)	L'organizzazione: a. Verifica che il sistema informativo sia in grado di eseguire l'auditing dei seguenti eventi: eventi di accesso all'account riusciti e non riusciti, eventi di gestione dell'account, accesso agli oggetti, modifica dei criteri, funzioni di privilegio, tracciamento dei processi ed eventi di sistema. Per le applicazioni web: tutte le attività dell'amministratore, i controlli di autenticazione, i controlli di autorizzazione, le eliminazioni di dati, l'accesso ai dati, le modifiche dei dati e le modifiche dei permessi. d. Stabilisce che i seguenti eventi devono essere sottoposti ad audit all'interno del sistema informativo: [sottoinsieme definito dall'organizzazione degli	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	eventi verificabili definiti in AU-2 a da verificare continuam ente per ogni evento identificato].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2(a)(d)	L'organizzazione: a. Verifica che il sistema informati vo sia in grado di eseguire l'auditing dei seguenti eventi: eventi di accesso all'account riusciti e non riusciti, eventi di gestione dell'account, accesso agli oggetti, modifica dei criteri, funzioni di privilegi o, tracciamento dei processi ed eventi di sistema. Per le applicazioni web: tutte le attività dell'ammi nistratore, i controlli di autenticazione, i controlli di autorizza zione, le eliminazioni di dati, l'accesso ai dati, le modifiche dei dati e le modifiche dei permessi. d. Stabilisc e che i seguenti eventi devono essere sottoposti ad audit all'interno del sistema informativo: [sottoins ieme definito dall'orga nizzazione degli	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	eventi verificabili definiti in AU-2 a da verificare continuamente per ogni evento identificato].		
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatc h Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazi oni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanismi automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizzativi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organizzazione analizza e mette in correlazione i record di audit in diversi repository per acquisire una conoscenza della situazione a livello di organizzazione.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanismi automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizzativi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organizzazione analizza e mette in correlazione i record di audit in diversi repository per acquisire una conoscenza della situazione a livello di organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanismi automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizzativi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organizzazione analizza e mette in correlazione i record di audit in diversi repository per acquisire una conoscenza della situazione a livello di organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indiriz zo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicaz ione centrale all'inter no di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettaglia te sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
AU-7(1)	Il sistema informati vo offre la capacità di elaborare record di audit per eventi di interesse sulla base di [Assegnazione: campi di audit definiti dall'organizzazione all'interno dei record di audit].	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-7(1)	Il sistema informativo offre la capacità di elaborare record di audit per eventi di interesse sulla base di [Assegnazione: campi di audit definiti dall'organizzazione all'interno dei record di audit].	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9(2)	Il sistema informativo esegue il backup dei record di audit almeno settimanalmente su un sistema o un componente del sistema fisicamente diverso dal sistema o dal componente sottoposto ad audit.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9(2)	Il sistema informativo esegue il backup dei record di audit almeno settimanalmente su un sistema o un componente del sistema fisicamente diverso dal sistema o dal componente sottoposto ad audit.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.
AU-9	Il sistema informativo protegge le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9	Il sistema informativo protegge le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9	Il sistema informativo protegge le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
AU-11	L'organizzazione conserva i registri di controllo per almeno 90 giorni per fornire supporto after-the-fact nelle indagini sugli incidenti di sicurezza e per soddisfare i requisiti normativi e organizzativi di conservazione delle informazioni.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Garantisce la capacità di generare record di audit per gli eventi verificabili definiti in AU-2 a. in tutti i componenti del sistema informativo e della rete in cui la capacità di audit è distribuita/disponibile c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Garantisce la capacità di generare record di audit per gli eventi verificabili definiti in AU-2 a. in tutti i componenti del sistema informativo e della rete in cui la capacità di audit è distribuita/disponibile c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Garantisce la capacità di generare record di audit per gli eventi verificabili definiti in AU-2 a. in tutti i componenti del sistema informativo e della rete in cui la capacità di audit è distribuita/disponibile c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Garantisce la capacità di generare record di audit per gli eventi verificabili definiti in AU-2 a. in tutti i componenti del sistema informativo e della rete in cui la capacità di audit è distribuita/disponibile c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Garantisce la capacità di generare record di audit per gli eventi verificabili definiti in AU-2 a. in tutti i componenti del sistema informativo e della rete in cui la capacità di audit è distribuita/disponibile c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AU-12(a)(c)	Il sistema informativo: a. Garantisce la capacità di generare record di audit per gli eventi verificabili definiti in AU-2 a. in tutti i componenti del sistema informativo e della rete in cui la capacità di audit è distribuita/disponibile c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Garantisce la capacità di generare record di audit per gli eventi verificabili definiti in AU-2 a. in tutti i componenti del sistema informativo e della rete in cui la capacità di audit è distribuita/disponibile c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Garantisce la capacità di generare record di audit per gli eventi verificabili definiti in AU-2 a. in tutti i componenti del sistema informativo e della rete in cui la capacità di audit è distribuita/disponibile c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Garantisce la capacità di generare record di audit per gli eventi verificabili definiti in AU-2 a. in tutti i componenti del sistema informativo e della rete in cui la capacità di audit è distribuita/disponibile c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Garantisce la capacità di generare record di audit per gli eventi verificabili definiti in AU-2 a. in tutti i componenti del sistema informativo e della rete in cui la capacità di audit è distribuita/disponibile c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Garantisce la capacità di generare record di audit per gli eventi verificabili definiti in AU-2 a. in tutti i componenti del sistema informativo e della rete in cui la capacità di audit è distribuita/disponibile c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Garantisce la capacità di generare record di audit per gli eventi verificabili definiti in AU-2 a. in tutti i componenti del sistema informativo e della rete in cui la capacità di audit è distribuita/disponibile c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	rds-enhanced-monit oring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorar e la disponibilità di Amazon RDS. Ciò fornisce una visibilit à dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archivi azione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositi vo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	beanstalk-enhanced -health-reporting- enabled	AWS La reportist ica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamen ti nello stato dell'infr astruttura sottostan te. Queste modifiche potrebbero comportar e una mancanza di disponibilità dell'appl icazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descritto re dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registran do le azioni della console di gestione e le chiamate API. È possibile identific are gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indiriz zo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	dynamodb-throughpu t-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissi one assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportar e. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficien ti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissi one effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltati vamente i parametri AccountRCU ThresholdPercentag e (Config Default: 80) e AccountWCU ThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitorag gio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-7(a)	L'organizzazione: a. Configura il sistema informativo per fornire solo le funzionalità essenziali.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.
CM-7(a)	L'organizzazione: a. Configura il sistema informativo per fornire solo le funzionalità essenziali.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-7(a)	L'organizzazione: a. Configura il sistema informativo per fornire solo le funzionalità essenziali.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(1)	L'organizzazione aggiorna l'inventario dei componenti del sistema informativo come parte integrante e delle installazioni dei componenti, delle rimozioni e degli aggiornamenti del sistema stesso.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(1)	L'organizzazione aggiorna l'inventario dei componenti del sistema informativo come parte integrante e delle installazioni dei componenti, delle rimozioni e degli aggiornamenti del sistema stesso.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(3)(a)	L'organizzazione: a. Impiega continuam ente meccanismi automatici, utilizzan do meccanismi automatici con un ritardo massimo di cinque minuti nel rilevamento, per rilevare la presenza di componenti hardware, software e firmware non autorizzati all'interno del sistema informativo.	ec2-instance-manag ed-by-systems-mana ger	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(3)(a)	L'organizzazione: a. Impiega continuam ente meccanismi automatici, utilizzan do meccanismi automatici con un ritardo massimo di cinque minuti nel rilevamento, per rilevare la presenza di componenti hardware, software e firmware non autorizzati all'interno del sistema informativo.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associati ons per semplific are l'inventario delle piattaforme e delle applicazioni software all'interno di un'organi zzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo , delle installaz ioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(3)(a)	L'organizzazione: a. Impiega continuam ente meccanismi automatici, utilizzan do meccanismi automatici con un ritardo massimo di cinque minuti nel rilevamento, per rilevare la presenza di componenti hardware, software e firmware non autorizzati all'interno del sistema informativo.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(3)(a)	L'organizzazione: a. Impiega continuam ente meccanismi automatici, utilizzan do meccanismi automatici con un ritardo massimo di cinque minuti nel rilevamento, per rilevare la presenza di componenti hardware, software e firmware non autorizzati all'interno del sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informativo (incrementali giornalieri; completi settimanalmente).	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informativo (incrementali giornalieri; completi settimanalmente).	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informati vo (incrementali giornalieri; completi settimanalmente).	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informativo (incrementali giornalieri; completi settimanalmente).	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informativo (incrementali giornalieri; completi settimanalmente).	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informativo (incrementali giornalieri; completi settimanalmente).	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informativo (incrementali giornalieri; completi settimanalmente).	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informativo (incrementali giornalieri; completi settimanalmente).	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informativo (incrementali giornalieri; completi settimanalmente).	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informativo (incrementali giornalieri; completi settimanalmente).	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informativo (incrementali giornalieri; completi settimanalmente).	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informati vo (incrementali giornalieri; completi settimanalmente).	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informativo (incrementali giornalieri; completi settimanalmente).	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9(b)	L'organizzazione: b. Esegue backup delle informazioni a livello di sistema contenute nel sistema informativo (incrementali giornalieri; completi settimanalmente).	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CP-10	L'organizzazione provvede al ripristin o e alla ricostituzione del sistema informati vo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(1)(2)	(1) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account con privilegi. (2) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account senza privilegi.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(1)(2)	(1) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account con privilegi. (2) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account senza privilegi.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(1)(2)	(1) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account con privilegi. (2) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account senza privilegi.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(1)(2)	(1) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account con privilegi. (2) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account senza privilegi.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(1)	(1) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account con privilegi.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(1)	(1) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account con privilegi.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione e alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(1)	(1) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account con privilegi.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(1)	(1) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account con privilegi.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2	Il sistema informativo identifica e autentica in modo univoco gli utenti dell'orga nizzazione (o i processi che agiscono per loro conto).	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2	Il sistema informativo identifica e autentica in modo univoco gli utenti dell'organizzazione (o i processi che agiscono per loro conto).	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-5(1)(a)(d)(e)	Il sistema informativo, per l'autenticazione basata su password: a. Applica una complessità minima della password di [Assegnazione: requisiti definiti dall'organizzazion e per la distinzio ne tra maiuscole e minuscole, numero di caratteri, combinazi one di lettere maiuscole, lettere minuscole, numeri e caratteri speciali, inclusi i requisiti minimi per ogni tipo]; d. Applica le restrizioni sulla durata minima e massima delle password di [Assegnazione: numeri definiti dall'organizzazione per la durata minima, durata massima]; e. Proibisce il riutilizzo delle password per 24 generazioni	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-5(4)	L'organizzazione utilizza strumenti automatizzati per determinare se gli autenticatori di password sono sufficientemente potenti da soddisfare [Assegnazione: requisiti definiti dall'organizzazione].	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-5(7)	L'organizzazione garantisce che gli autenticatori statici non crittografati non vengano incorporati nelle applicazioni o negli script di accesso o memorizzati nei tasti funzione.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-4(1)	L'organizzazione utilizza meccanism i automatizzati per supportare il processo di gestione degli incidenti.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-4(1)	L'organizzazione utilizza meccanism i automatizzati per supportare il processo di gestione degli incidenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-4(1)	L'organizzazione utilizza meccanismi automatizzati per supportare il processo di gestione degli incidenti.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-4(1)	L'organizzazione utilizza meccanism i automatizzati per supportare il processo di gestione degli incidenti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-4(1)	L'organizzazione utilizza meccanism i automatizzati per supportare il processo di gestione degli incidenti.	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-6(1)	L'organizzazione utilizza meccanism i automatizzati per facilitare la segnalazi one degli incidenti di sicurezza.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-6(1)	L'organizzazione utilizza meccanismi automatizzati per facilitare la segnalazione degli incidenti di sicurezza.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-6(1)	L'organizzazione utilizza meccanism i automatizzati per facilitare la segnalazi one degli incidenti di sicurezza.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-7(1)	L'organizzazione utilizza meccanism i automatizzati per aumentare la disponibilità di informazioni e supporto relativi alla risposta agli incidenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-7(1)	L'organizzazione utilizza meccanismi automatizzati per aumentare la disponibilità di informazioni e supporto relativi alla risposta agli incidenti.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-7(1)	L'organizzazione utilizza meccanism i automatizzati per aumentare la disponibilità di informazioni e supporto relativi alla risposta agli incidenti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA-5(1)	L'organizzazione utilizza strumenti di scansione delle vulnerabilità che includono la capacità di aggiornare prontamente le vulnerabilità del sistema informati vo da scansionare. Guida supplemen tare: i punti vulnerabi li da sottoporre a scansione devono essere prontamen te aggiornati man mano che vengono scoperte, annunciat e e sviluppate nuove vulnerabilità e metodi di scansione . Questo processo di aggiornamento aiuta a garantire che le potenziali vulnerabilità del sistema informati vo siano identific ate e affrontate il più rapidamente possibile . Controlli correlati: SI-3, SI-7.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA-5(1)	L'organizzazione utilizza strumenti di scansione delle vulnerabilità che includono la capacità di aggiornare prontamente le vulnerabilità del sistema informativo da scansionare. Guida supplementare: i punti vulnerabili da sottoporre a scansione devono essere prontamente aggiornati man mano che vengono scoperte, annunciate e sviluppate nuove vulnerabilità e metodi di scansione. Questo processo di aggiornamento aiuta a garantire che le potenziali vulnerabilità del sistema informativo siano identificate e affrontate il più rapidamente possibile. Controlli correlati: SI-3, SI-7.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA-5(1)	L'organizzazione utilizza strumenti di scansione delle vulnerabilità che includono la capacità di aggiornare prontamente le vulnerabilità del sistema informati vo da scansionare. Guida supplemen tare: i punti vulnerabi li da sottoporre a scansione devono essere prontamen te aggiornati man mano che vengono scoperte, annunciat e e sviluppate nuove vulnerabilità e metodi di scansione . Questo processo di aggiornamento aiuta a garantire che le potenziali vulnerabilità del sistema informati vo siano identific ate e affrontate il più rapidamente possibile . Controlli correlati: SI-3, SI-7.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA-5	L'organizzazione: a. Scansiona mensilmente le vulnerabilità del sistema informativo e delle applicazioni ospitate [sistema operativo/infrastruttura; mensilmente applicazioni web e database] e quando vengono identificate e segnalate nuove vulnerabilità che potrebbero interessare il sistema/le applicazioni; b. Utilizza strumenti e tecniche di scansione delle vulnerabilità che facilitano l'interoperabilità tra gli strumenti e automatizzano parti del processo di gestione delle vulnerabilità utilizzando standard per: 1. Enumerazione di piattaforme, difetti del software e configurazioni improprie; 2. Formattazione di liste di controllo e	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	procedure di test; e 3. Misurazione dell'impatto delle vulnerabilità; c. Analizza i report di scansione delle vulnerabilità e i risultati delle valutazioni del controllo di sicurezza; d. Rimedi alle vulnerabilità legittime: vulnerabilità ad alto rischio mitigate entro trenta (30) giorni dalla data di scoperta; vulnerabilità a rischio moderato mitigate entro novanta (90) giorni dalla data di scoperta; vulnerabilità a basso rischio mitigate entro centottanta (180) giorni dalla data di scoperta, conformemente a una valutazione organizzativa del rischio; e. Condivide le informazioni ottenute dal processo di scansione delle vulnerabilità e dalle valutazioni del controllo della sicurezza con		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	[Assegnazione: personale o ruoli definiti dall'orga nizzazione] per aiutare a eliminare vulnerabilità simili in altri sistemi informativi (ad esempio, criticità o carenze sistemich e).		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA-5	L'organizzazione: a. Esegue la scansione delle vulnerabilità nel sistema informativo e nelle applicazioni ospitate [Assegnazione: frequenza definita dall'organizzazione e/o in modo casuale in base al processo definito dall'organizzazione] e quando vengono identificate e segnalate nuove vulnerabilità che potrebbero influire sul sistema/sulle applicazioni; b. Utilizza strumenti e tecniche di scansione delle vulnerabilità che facilitano l'interoperabilità tra gli strumenti e automatizzano parti del processo di gestione delle vulnerabilità utilizzando standard per: 1. Enumerazione di piattaforme, difetti del software e configura	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	zioni improprie; 2. Formattazione di liste di controllo e procedure di test; e 3. Misurazione dell'impatto delle vulnerabilità; c. Analizza i report di scansione delle vulnerabilità e i risultati delle valutazioni del controllo di sicurezza; d. Corregge le vulnerabilità legittime [Assegnazione: tempi di risposta definiti dall'organizzazione], secondo una valutazione del rischio dell'organizzazione; e. Condivide le informazioni ottenute dal processo di scansione delle vulnerabilità e dalle valutazioni del controllo della sicurezza con [Assegnazione: personale o ruoli definiti dall'organizzazione] per aiutare a eliminare vulnerabilità simili in altri sistemi informativi		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(ad esempio, criticità o carenze sistemiche).		
SA-3(a)	L'organizzazione: a. Gestisce il sistema informativo utilizzando [Assegnazione: ciclo di vita dello sviluppo del sistema definito dall'organizzazione] che incorpora considerazioni sulla sicurezza delle informazioni.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-3(a)	L'organizzazione: a. Gestisce il sistema informativo utilizzando [Assegnazione: ciclo di vita dello sviluppo del sistema definito dall'organizzazione] che incorpora considerazioni sulla sicurezza delle informazioni.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-3(a)	L'organizzazione: a. Gestisce il sistema informativo utilizzando [Assegnazione: ciclo di vita dello sviluppo del sistema definito dall'organizzazione] che incorpora considerazioni sulla sicurezza delle informazioni.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-10	L'organizzazione richiede allo sviluppatore del sistema informativo, del componente del sistema o del servizio del sistema informativo di: a. Eseguire la gestione della configurazione durante lo sviluppo, l'implementazione e il funzionamento di sistemi, componenti o servizi; b. Documentare, gestire e controllare l'integrità delle modifiche a [Assegnazione: elementi di configurazione definiti dall'organizzazione nell'ambito della gestione della configurazione]; c. Implementare solo le modifiche al sistema, al componente o al servizio approvate dall'organizzazione; d. Documentare le modifiche al sistema, al componente o al servizio approvate	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e i potenziali impatti sulla sicurezza di tali modifiche; e. Tieni traccia dei difetti di sicurezza e della risoluzione dei difetti all'interno del sistema, del componente o del servizio e segnala i risultati a [Assegnazione: personale definito dall'organizzazione].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-10	L'organizzazione richiede allo sviluppatore del sistema informativo, del componente del sistema o del servizio del sistema informativo di: a. Eseguire la gestione della configurazione durante lo sviluppo, l'implementazione e il funzionamento di sistemi, componenti o servizi; b. Documentare, gestire e controllare l'integrità delle modifiche a [Assegnazione: elementi di configurazione definiti dall'organizzazione nell'ambito della gestione della configurazione]; c. Implementare solo le modifiche al sistema, al componente o al servizio approvate dall'organizzazione; d. Documentare le modifiche al sistema, al componente o al servizio approvate	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e i potenziali impatti sulla sicurezza di tali modifiche; e. Tieni traccia dei difetti di sicurezza e della risoluzione dei difetti all'interno del sistema, del componente o del servizio e segnala i risultati a [Assegnazione: personale definito dall'organizzazione].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-10	L'organizzazione richiede allo sviluppatore del sistema informativo, del componente del sistema o del servizio del sistema informativo di: a. Eseguire la gestione della configurazione durante lo sviluppo, l'implementazione e il funzionamento di sistemi, componenti o servizi; b. Documentare, gestire e controllare l'integrità delle modifiche a [Assegnazione: elementi di configurazione definiti dall'organizzazione nell'ambito della gestione della configurazione]; c. Implementare solo le modifiche al sistema, al componente o al servizio approvate dall'organizzazione; d. Documentare le modifiche al sistema, al componente o al servizio approvate	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e i potenziali impatti sulla sicurezza di tali modifiche; e. Tieni traccia dei difetti di sicurezza e della risoluzione dei difetti all'interno del sistema, del componente o del servizio e segnala i risultati a [Assegnazione: personale definito dall'organizzazione].		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-10	L'organizzazione richiede allo sviluppatore del sistema informativo, del componente del sistema o del servizio del sistema informativo di: a. Eseguire la gestione della configurazione durante lo sviluppo, l'implementazione e il funzionamento di sistemi, componenti o servizi; b. Documentare, gestire e controllare l'integrità delle modifiche a [Assegnazione: elementi di configurazione definiti dall'organizzazione nell'ambito della gestione della configurazione]; c. Implementare solo le modifiche al sistema, al componente o al servizio approvate dall'organizzazione; d. Documentare le modifiche al sistema, al componente o al servizio approvate	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e i potenziali impatti sulla sicurezza di tali modifiche; e. Tieni traccia dei difetti di sicurezza e della risoluzione dei difetti all'interno del sistema, del componente o del servizio e segnala i risultati a [Assegnazione: personale definito dall'organizzazione].		
SC-2	Il sistema informativo separa la funzionalità utente (compresi i servizi di interfaccia utente) dalla funzionalità di gestione del sistema informativo.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-2	Il sistema informativo separa la funzionalità utente (compresi i servizi di interfaccia utente) dalla funzionalità di gestione del sistema informativo.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
SC-2	Il sistema informativo separa la funzionalità utente (compresi i servizi di interfaccia utente) dalla funzionalità di gestione del sistema informativo.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-2	Il sistema informativo separa la funzionalità utente (compresi i servizi di interfaccia utente) dalla funzionalità di gestione del sistema informativo.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-2	Il sistema informativo separa la funzionalità utente (compresi i servizi di interfaccia utente) dalla funzionalità di gestione del sistema informativo.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	L'organizzazione: (a) implementa un'interf accia gestita per ogni servizio di telecomun icazione esterno; (b) stabilisce una policy di flusso del traffico per ogni interfaccia gestita; (c) protegge la riservatezza e l'integri tà delle informazioni trasmesse attravers o ogni interfaccia; (d) documenta ogni eccezione alla policy di flusso del traffico con un'esigenza di missione/azienda di supporto e la durata di tale esigenza; e (e) rivede le eccezioni alla policy di flusso del traffico [assegnaz ione: frequenza definita dall'orga nizzazione] e rimuove le eccezioni che non sono più supportat e da un'esplicita esigenza di missione/ azienda. Guida supplementare:	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Controllo correlato: SC-8.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	L'organizzazione: (a) implementa un'interfaccia gestita per ogni servizio di telecomunicazione esterno; (b) stabilisce una policy di flusso del traffico per ogni interfaccia gestita; (c) protegge la riservatezza e l'integrità delle informazioni trasmesse attraverso ogni interfaccia; (d) documenta ogni eccezione alla policy di flusso del traffico con un'esigenza di missione/azienda di supporto e la durata di tale esigenza; e (e) rivede le eccezioni alla policy di flusso del traffico [assegnazione: frequenza definita dall'organizzazione] e rimuove le eccezioni che non sono più supportate da un'esplicita esigenza di missione/azienda. Guida supplementare:	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Controllo correlato: SC-8.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	L'organizzazione: (a) implementa un'interf accia gestita per ogni servizio di telecomun icazione esterno; (b) stabilisce una policy di flusso del traffico per ogni interfaccia gestita; (c) protegge la riservatezza e l'integri tà delle informazioni trasmesse attravers o ogni interfaccia; (d) documenta ogni eccezione alla policy di flusso del traffico con un'esigenza di missione/azienda di supporto e la durata di tale esigenza; e (e) rivede le eccezioni alla policy di flusso del traffico [assegnaz ione: frequenza definita dall'orga nizzazione] e rimuove le eccezioni che non sono più supportat e da un'esplicita esigenza di missione/ azienda. Guida supplementare:	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Controllo correlato: SC-8.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	L'organizzazione: (a) implementa un'interf accia gestita per ogni servizio di telecomun icazione esterno; (b) stabilisce una policy di flusso del traffico per ogni interfaccia gestita; (c) protegge la riservatezza e l'integri tà delle informazioni trasmesse attravers o ogni interfaccia; (d) documenta ogni eccezione alla policy di flusso del traffico con un'esigenza di missione/azienda di supporto e la durata di tale esigenza; e (e) rivede le eccezioni alla policy di flusso del traffico [assegnaz ione: frequenza definita dall'orga nizzazione] e rimuove le eccezioni che non sono più supportat e da un'esplicita esigenza di missione/ azienda. Guida supplementare:	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Controllo correlato: SC-8.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	L'organizzazione: (a) implementa un'interf accia gestita per ogni servizio di telecomun icazione esterno; (b) stabilisce una policy di flusso del traffico per ogni interfaccia gestita; (c) protegge la riservatezza e l'integri tà delle informazioni trasmesse attravers o ogni interfaccia; (d) documenta ogni eccezione alla policy di flusso del traffico con un'esigenza di missione/azienda di supporto e la durata di tale esigenza; e (e) rivede le eccezioni alla policy di flusso del traffico [assegnaz ione: frequenza definita dall'orga nizzazione] e rimuove le eccezioni che non sono più supportat e da un'esplicita esigenza di missione/ azienda. Guida supplementare:	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Controllo correlato: SC-8.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	L'organizzazione: (a) implementa un'interf accia gestita per ogni servizio di telecomun icazione esterno; (b) stabilisce una policy di flusso del traffico per ogni interfaccia gestita; (c) protegge la riservatezza e l'integri tà delle informazioni trasmesse attravers o ogni interfaccia; (d) documenta ogni eccezione alla policy di flusso del traffico con un'esigenza di missione/azienda di supporto e la durata di tale esigenza; e (e) rivede le eccezioni alla policy di flusso del traffico [assegnaz ione: frequenza definita dall'orga nizzazione] e rimuove le eccezioni che non sono più supportat e da un'esplicita esigenza di missione/ azienda. Guida supplementare:	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Controllo correlato: SC-8.		
SC-7(5)	Il sistema informativo sulle interfacce gestite nega il traffico delle comunicazioni di rete per impostazione predefinita e consente il traffico delle comunicazioni di rete per eccezione (cioè, negare tutto, consentire per eccezione). Guida supplementare: questo miglioramento del controllo si applica al traffico di comunicazione di rete in entrata e in uscita. Una politica di negazione totale del traffico delle comunicazioni di permit-by-exception rete garantisce che siano consentite solo le connessioni essenziali e approvate.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8	Il sistema informativo protegge la riservatezza e l'integrità delle informazioni trasmesse.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8	Il sistema informativo protegge la riservatezza e l'integrità delle informazioni trasmesse.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-8	Il sistema informativo protegge la riservatezza e l'integrità delle informazioni trasmesse.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8	Il sistema informativo protegge la riservatezza e l'integrità delle informazioni trasmesse.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8	Il sistema informativo protegge la riservatezza e l'integrità delle informazioni trasmesse.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8	Il sistema informativo protegge la riservatezza e l'integrità delle informazioni trasmesse.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8	Il sistema informativo protegge la riservatezza e l'integrità delle informazioni trasmesse.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12	L'organizzazione stabilisce e gestisce le chiavi crittografiche per la crittografia richiesta impiegata all'interno del sistema informativo in conformità a [Assegnazione: requisiti definiti dall'organizzazione per la generazione, la distribuzione, l'archiviazione e la distruzione delle chiavi e l'accesso alle stesse].	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12	L'organizzazione stabilisce e gestisce le chiavi crittografiche per la crittografia richiesta impiegata all'interno del sistema informativo in conformità a [Assegnazione: requisiti definiti dall'organizzazione per la generazione, la distribuzione, l'archiviazione e la distruzione delle chiavi e l'accesso alle stesse].	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12	L'organizzazione stabilisce e gestisce le chiavi crittografiche per la crittografia richiesta impiegata all'interno del sistema informativo in conformità a [Assegnazione: requisiti definiti dall'organizzazione per la generazione, la distribuzione, l'archiviazione e la distruzione delle chiavi e l'accesso alle stesse].	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Il sistema informativo implementa la crittografia convalidata da FIPS o approvata da NSA in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel servizio di gestione delle AWS chiavi (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Il sistema informati vo implement a la crittografia convalidata da FIPS o approvata da NSA in conformità alle leggi federali applicabili, agli ordini esecutivi , alle direttive, alle policy, ai regolamenti e agli standard.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
SC-13	Il sistema informati vo implement a la crittografia convalidata da FIPS o approvata da NSA in conformità alle leggi federali applicabili, agli ordini esecutivi , alle direttive, alle policy, ai regolamenti e agli standard.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Managemen t Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché nell' SageMaker endpoint possono esistere dati sensibili inattivi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Il sistema informati vo implement a la crittografia convalidata da FIPS o approvata da NSA in conformità alle leggi federali applicabili, agli ordini esecutivi , alle direttive, alle policy, ai regolamenti e agli standard.	sagemaker-notebook -instance-kms-key- configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Il sistema informativo implementa la crittografia convalidata da FIPS o approvata da NSA in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
SC-13	Il sistema informativo implementa la crittografia convalidata da FIPS o approvata da NSA in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23	Il sistema informativo protegge l'autenticità delle sessioni di comunicazione.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-23	Il sistema informativo protegge l'autenticità delle sessioni di comunicazione.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23	Il sistema informativo protegge l'autenticità delle sessioni di comunicazione.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-23	Il sistema informativo protegge l'autenticità delle sessioni di comunicazione.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23	Il sistema informativo protegge l'autenticità delle sessioni di comunicazione.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-23	Il sistema informativo protegge l'autenticità delle sessioni di comunicazione.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Il sistema informativo protegge la riservatezza E l'integrità di [Assegnazione: informazioni a riposo definite dall'organizzazione].	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché nell' SageMaker endpoint possono esistere dati sensibili inattivi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(2)	L'organizzazione impiega meccanismi automatizzati almeno mensilmente per determinare lo stato dei componenti del sistema informativo in relazione alla correzione dei difetti.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(2)	L'organizzazione impiega meccanismi automatizzati almeno mensilmente per determinare lo stato dei componenti del sistema informativo in relazione alla correzione dei difetti.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(2)	L'organizzazione impiega meccanismi automatizzati almeno mensilmente per determinare lo stato dei componenti del sistema informati vo in relazione alla correzione dei difetti.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(2)	L'organizzazione impiega meccanismi automatizzati almeno mensilmente per determinare lo stato dei componenti del sistema informati vo in relazione alla correzione dei difetti.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3	L'organizzazione: a. Impiega meccanism i di protezione da codice maligno nei punti di ingresso e di uscita del sistema informativo per rilevare ed eliminare il codice dannoso; b. Aggiorna i meccanism i di protezione da codice dannoso ogni volta che sono disponibili nuovi rilasci, conformem ente alla policy e alle procedure di gestione della configurazione dell'organizzazion e; c. Configura i meccanismi di protezione da codice dannoso per: 1. Eseguire scansioni periodiche del sistema informati vo [Assegnazione: frequenza definita dall'organizzazione] e scansioni in tempo reale di file provenien ti da fonti esterne presso [Selezione	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCES S_KEY_ID e AWS_SECRE T_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(uno o più); endpoint; punti di ingresso/ uscita dalla rete] nel momento in cui i file vengono scaricati , aperti o eseguiti, in conformità alla policy di sicurezza dell'organizzazione; e 2. [Selezione (una o più): bloccare il codice maligno; mettere in quarantena il codice dannoso; inviare un avviso all'ammin istratore; [Assegnaz ione: azione definita dall'organizzazion e]] in risposta al rilevamento di codice maligno; e d. Affronta la ricezione di falsi positivi durante il rilevamento e l'eliminazione di codici dannoso e il conseguente impatto potenzial e sulla disponibi lità del sistema informativo. Guida supplementare: i punti di ingresso e di uscita del sistema informati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	vo comprendono, ad esempio, firewall, server di posta elettronica, server web, server proxy, server di accesso remoto, workstation, notebook e dispositi vi mobili. Il codice dannoso comprende , ad esempio, virus, worm, cavalli di Troia e spyware. Il codice dannoso può anche essere codificato in vari formati (ad esempio, UUENCODE, Unicode), contenuto in file compressi o nascosti o nascosto in file utilizzando la steganografia. Il codice dannoso può essere trasportato con diversi mezzi, tra cui, ad esempio, accessi al web, posta elettroni ca, allegati di posta elettronica e dispositi vi di archiviazione portatili. L'inserimento di codice dannoso avviene attravers		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	o lo sfruttamento delle vulnerabilità del sistema informati co. I meccanismi di protezione dal codice dannoso includono , ad esempio, le definizioni delle firme antivirus e le tecnologi e basate sulla reputazione. Esistono diverse tecnologie e metodi per limitare o eliminare gli effetti del codice dannoso. Una gestione pervasiva della configurazione e controlli completi dell'integrità del software possono essere efficaci nel prevenire l'esecuzi one di codice non autorizzato. Oltre al off-the-shelf software commerciale, il codice dannoso può essere presente anche nel software personalizzato. Ciò potrebbe includere , ad esempio, bombe logiche, backdoor e altri tipi		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di attacchi informati ci che potrebber o compromet tere le missioni/ funzioni aziendali dell'organizzazione. I meccanismi tradizion ali di protezione del codice dannoso non sono sempre in grado di rilevare questo tipo di codice. In queste situazion i, le organizzazioni si affidano invece ad altre misure di protezione, tra cui, ad esempio, pratiche di codifica sicure, gestione e controllo della configurazione, processi di approvvig ionamento affidabili e pratiche di monitorag gio per garantire che il software non svolga funzioni diverse da quelle previste. Le organizzazioni possono stabilire che, in risposta al rilevamento di codice dannoso, possono essere giustificate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	azioni diverse. Ad esempio, le organizzazioni possono definire azioni in risposta al rilevamento di codice dannoso durante le scansioni periodiche, azioni in risposta al rilevamento di download dannosi e/o azioni in risposta al rilevamento di malware quando si tenta di aprire o eseguire file. Controlli correlati: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Riferimenti: Pubblicazione speciale NIST 800-83.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3	L'organizzazione: a. Impiega meccanism i di protezione da codice maligno nei punti di ingresso e di uscita del sistema informativo per rilevare ed eliminare il codice dannoso; b. Aggiorna i meccanism i di protezione da codice dannoso ogni volta che sono disponibili nuovi rilasci, conformem ente alla policy e alle procedure di gestione della configurazione dell'organizzazion e; c. Configura i meccanismi di protezione da codice dannoso per: 1. Eseguire scansioni periodiche del sistema informati vo [Assegnazione: frequenza definita dall'organizzazione] e scansioni in tempo reale di file provenien ti da fonti esterne presso [Selezione	codebuild-project-source-repo-url-check	Assicurati che l' GitHub URL del repository di origine di Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(uno o più); endpoint; punti di ingresso/ uscita dalla rete] nel momento in cui i file vengono scaricati , aperti o eseguiti, in conformità alla policy di sicurezza dell'organizzazione; e 2. [Selezione (una o più): bloccare il codice maligno; mettere in quarantena il codice dannoso; inviare un avviso all'ammin istratore; [Assegnaz ione: azione definita dall'organizzazion e]] in risposta al rilevamento di codice maligno; e d. Affronta la ricezione di falsi positivi durante il rilevamento e l'eliminazione di codici dannoso e il conseguente impatto potenzial e sulla disponibi lità del sistema informativo. Guida supplementare: i punti di ingresso e di uscita del sistema informati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	vo comprendono, ad esempio, firewall, server di posta elettronica, server web, server proxy, server di accesso remoto, workstation, notebook e dispositi vi mobili. Il codice dannoso comprende , ad esempio, virus, worm, cavalli di Troia e spyware. Il codice dannoso può anche essere codificato in vari formati (ad esempio, UUENCODE, Unicode), contenuto in file compressi o nascosti o nascosto in file utilizzando la steganografia. Il codice dannoso può essere trasportato con diversi mezzi, tra cui, ad esempio, accessi al web, posta elettroni ca, allegati di posta elettronica e dispositi vi di archiviazione portatili. L'inserimento di codice dannoso avviene attravers		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	o lo sfruttamento delle vulnerabilità del sistema informati co. I meccanismi di protezione dal codice dannoso includono , ad esempio, le definizioni delle firme antivirus e le tecnologi e basate sulla reputazione. Esistono diverse tecnologie e metodi per limitare o eliminare gli effetti del codice dannoso. Una gestione pervasiva della configurazione e controlli completi dell'integrità del software possono essere efficaci nel prevenire l'esecuzi one di codice non autorizzato. Oltre al off-the-shelf software commerciale, il codice dannoso può essere presente anche nel software personalizzato. Ciò potrebbe includere , ad esempio, bombe logiche, backdoor e altri tipi		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di attacchi informati ci che potrebber o compromet tere le missioni/ funzioni aziendali dell'organizzazione. I meccanismi tradizion ali di protezione del codice dannoso non sono sempre in grado di rilevare questo tipo di codice. In queste situazion i, le organizzazioni si affidano invece ad altre misure di protezione, tra cui, ad esempio, pratiche di codifica sicure, gestione e controllo della configurazione, processi di approvvig ionamento affidabili e pratiche di monitorag gio per garantire che il software non svolga funzioni diverse da quelle previste. Le organizzazioni possono stabilire che, in risposta al rilevamento di codice dannoso, possono essere giustificate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	azioni diverse. Ad esempio, le organizzazioni possono definire azioni in risposta al rilevamento di codice dannoso durante le scansioni periodiche, azioni in risposta al rilevamento di download dannosi e/o azioni in risposta al rilevamento di malware quando si tenta di aprire o eseguire file. Controlli correlati: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Riferimenti: Pubblicazione speciale NIST 800-83.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3	L'organizzazione: a. Impiega meccanism i di protezione da codice maligno nei punti di ingresso e di uscita del sistema informativo per rilevare ed eliminare il codice dannoso; b. Aggiorna i meccanism i di protezione da codice dannoso ogni volta che sono disponibili nuovi rilasci, conformem ente alla policy e alle procedure di gestione della configurazione dell'organizzazion e; c. Configura i meccanismi di protezione da codice dannoso per: 1. Eseguire scansioni periodiche del sistema informati vo [Assegnazione: frequenza definita dall'organizzazione] e scansioni in tempo reale di file provenien ti da fonti esterne presso [Selezione	ecs-task-definition-memory-hard-limit	La limitazione della memoria massima disponibile per i container Amazon Elastic Container Service (ECS) garantisce che l'utilizz o delle risorse non possa essere abusato in caso di accesso malevolo ai container.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(uno o più); endpoint; punti di ingresso/ uscita dalla rete] nel momento in cui i file vengono scaricati , aperti o eseguiti, in conformità alla policy di sicurezza dell'organizzazione; e 2. [Selezione (una o più): bloccare il codice maligno; mettere in quarantena il codice dannoso; inviare un avviso all'ammin istratore; [Assegnaz ione: azione definita dall'organizzazion e]] in risposta al rilevamento di codice maligno; e d. Affronta la ricezione di falsi positivi durante il rilevamento e l'eliminazione di codici dannoso e il conseguente impatto potenzial e sulla disponibi lità del sistema informativo. Guida supplementare: i punti di ingresso e di uscita del sistema informati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	vo comprendono, ad esempio, firewall, server di posta elettronica, server web, server proxy, server di accesso remoto, workstation, notebook e dispositi vi mobili. Il codice dannoso comprende , ad esempio, virus, worm, cavalli di Troia e spyware. Il codice dannoso può anche essere codificato in vari formati (ad esempio, UUENCODE, Unicode), contenuto in file compressi o nascosti in file mediante steganogr afia. Il codice dannoso può essere trasporta to con diversi mezzi, tra cui, ad esempio, accessi al web, posta elettronica, allegati di posta elettroni ca e dispositivi di archiviazione portatili . L'inserimento di codice dannoso avviene attravers		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	o lo sfruttamento delle vulnerabilità del sistema informati co. I meccanismi di protezione dal codice dannoso includono , ad esempio, le definizioni delle firme antivirus e le tecnologi e basate sulla reputazione. Esistono diverse tecnologie e metodi per limitare o eliminare gli effetti del codice dannoso. Una gestione pervasiva della configurazione e controlli completi dell'integrità del software possono essere efficaci nel prevenire l'esecuzi one di codice non autorizzato. Oltre al off-the-shelf software commerciale, il codice dannoso può essere presente anche nel software personalizzato. Ciò potrebbe includere , ad esempio, bombe logiche, backdoor e altri tipi		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di attacchi informati ci che potrebber o compromet tere le missioni/ funzioni aziendali dell'organizzazione. I meccanismi tradizion ali di protezione del codice dannoso non sono sempre in grado di rilevare questo tipo di codice. In queste situazion i, le organizzazioni si affidano invece ad altre misure di protezione, tra cui, ad esempio, pratiche di codifica sicure, gestione e controllo della configurazione, processi di approvvig ionamento affidabili e pratiche di monitorag gio per garantire che il software non svolga funzioni diverse da quelle previste. Le organizzazioni possono stabilire che, in risposta al rilevamento di codice dannoso, possono essere giustificate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	azioni diverse. Ad esempio, le organizzazioni possono definire azioni in risposta al rilevamento di codice dannoso durante le scansioni periodiche, azioni in risposta al rilevamento di download dannosi e/o azioni in risposta al rilevamento di malware quando si tenta di aprire o eseguire file. Controlli correlati: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Riferimenti: Pubblicazione speciale NIST 800-83.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(1)	L'organizzazione collega e configura i singoli strumenti di rilevamento delle intrusioni in un sistema di rilevamento delle intrusioni a livello di sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(4)	Il sistema informativo monitora costantem ente il traffico delle comunicazioni in entrata e in uscita per individuare attività o condizioni insolite o non autorizzate.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(4)	Il sistema informativo monitora costantemente il traffico delle comunicazioni in entrata e in uscita per individuare attività o condizioni insolite o non autorizzate.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(4)	Il sistema informativo monitora costantemente il traffico delle comunicazioni in entrata e in uscita per individuare attività o condizioni insolite o non autorizzate.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(4)	Il sistema informativo monitora costantem ente il traffico delle comunicazioni in entrata e in uscita per individuare attività o condizioni insolite o non autorizzate.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(5)	Il sistema informativo avvisa [Assegnazione: personale o ruoli definiti dall'organizzazione] quando si presentano le seguenti indicazioni di compromissione o potenziale compromissione: [Assegnazione: indicatori di compromissione definiti dall'organizzazione].	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(5)	Il sistema informativo avvisa [Assegnazione: personale o ruoli definiti dall'organizzazione] quando si presentano le seguenti indicazioni di compromissione o potenziale compromissione: [Assegnazione: indicatori di compromissione definiti dall'organizzazione].	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(5)	Il sistema informativo avvisa [Assegnazione: personale o ruoli definiti dall'organizzazione] quando si presentano le seguenti indicazioni di compromissione o potenziale compromissione: [Assegnazione: indicatori di compromissione definiti dall'organizzazione].	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(5)	Il sistema informativo avvisa [Assegnazione: personale o ruoli definiti dall'organizzazione] quando si presentano le seguenti indicazioni di compromissione o potenziale compromissione: [Assegnazione: indicatori di compromissione definiti dall'organizzazione].	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(16)	L'organizzazione mette in correlazione le informazioni provenienti dagli strumenti di monitoraggio utilizzati in tutto il sistema informativo.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(16)	L'organizzazione mette in correlazi one le informazioni provenienti dagli strumenti di monitorag gio utilizzati in tutto il sistema informativo.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(16)	L'organizzazione mette in correlazione le informazioni provenienti dagli strumenti di monitoraggio utilizzati in tutto il sistema informativo.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
SI-4(16)	L'organizzazione mette in correlazione le informazioni provenienti dagli strumenti di monitoraggio utilizzati in tutto il sistema informativo.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(16)	L'organizzazione mette in correlazi one le informazioni provenienti dagli strumenti di monitorag gio utilizzati in tutto il sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(16)	L'organizzazione mette in correlazione le informazioni provenienti dagli strumenti di monitoraggio utilizzati in tutto il sistema informativo.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi in conformit à a [Assegnazione: obiettivi di monitorag gio definiti dall'orga nizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnaz ione: tecniche e metodi definiti dall'organizzazion e]; c. Implement a dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazi oni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi in conformit à a [Assegnazione: obiettivi di monitorag gio definiti dall'orga nizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnaz ione: tecniche e metodi definiti dall'organizzazion e]; c. Implement a dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazi oni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenziali attacchi in conformità a [Assegnazione: obiettivi di monitoraggio definiti dall'organizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnazione: tecniche e metodi definiti dall'organizzazione]; c. Implementa dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazioni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenziali attacchi in conformità a [Assegnazione: obiettivi di monitoraggio definiti dall'organizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnazione: tecniche e metodi definiti dall'organizzazione]; c. Implementa dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazioni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenziali attacchi in conformità a [Assegnazione: obiettivi di monitoraggio definiti dall'organizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnazione: tecniche e metodi definiti dall'organizzazione]; c. Implementa dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazioni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi in conformit à a [Assegnazione: obiettivi di monitorag gio definiti dall'orga nizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnaz ione: tecniche e metodi definiti dall'organizzazion e]; c. Implement a dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazi oni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi in conformit à a [Assegnazione: obiettivi di monitorag gio definiti dall'orga nizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnaz ione: tecniche e metodi definiti dall'organizzazion e]; c. Implement a dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazi oni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi in conformit à a [Assegnazione: obiettivi di monitorag gio definiti dall'orga nizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnaz ione: tecniche e metodi definiti dall'organizzazion e]; c. Implement a dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazi oni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitorag gio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi in conformit à a [Assegnazione: obiettivi di monitorag gio definiti dall'orga nizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnaz ione: tecniche e metodi definiti dall'organizzazion e]; c. Implement a dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazi oni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-5	L'organizzazione: a. Riceve costantemente avvisi, consigli e direttive sulla sicurezza dei sistemi informativi da [Assegnazione: organizzazioni esterne definite dall'organizzazione]; b. Genera avvisi, consigli e direttive di sicurezza interna, se ritenuto necessario; c. Diffonde avvisi, consigli e direttive di sicurezza a: [Selezione (una o più): [Assegnazione: personale o ruoli definiti dall'organizzazione]; [Assegnazione: elementi definiti dall'organizzazione all'interno dell'organizzazione]; [Assegnazione: organizzazioni esterne definite dall'organizzazione]]; e d. Implementa le direttive di sicurezza	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	secondo le tempistic he stabilite o notifica all'organizzazione emittente il grado di non conformità. Guida supplemen tare: lo United States Computer Emergency Readiness Team (US-CERT) genera avvisi e consigli di sicurezza per mantenere la consapevolezza della situazione in tutto il governo federale. Le direttive di sicurezza sono emesse dall'OMB o da altre organizza zioni designate con la responsab ilità e l'autorità di emettere tali direttive . La conformità alle direttive di sicurezza è essenziale a causa della natura critica di molte di esse e dei potenziali effetti negativi immediati sulle operazioni e sui beni dell'orga nizzazione, sulle persone, sulle altre		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	organizzazioni e sulla Nazione, qualora le direttive non vengano implementate in modo tempestivo. Le organizzazioni esterne comprendo no, ad esempio, partner esterni di missione/azienda, partner della catena di fornitura, fornitori di servizi esterni e altre organizzazioni di pari livello/supporto. Controllo correlato : SI-2. Riferimen ti: Pubblicazione speciale NIST 800-40.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-5	L'organizzazione: a. Riceve costantemente avvisi, consigli e direttive sulla sicurezza dei sistemi informativi da [Assegnazione: organizzazioni esterne definite dall'organizzazione]; b. Genera avvisi, consigli e direttive di sicurezza interna, se ritenuto necessario; c. Diffonde avvisi, consigli e direttive di sicurezza a: [Selezione (una o più): [Assegnazione: personale o ruoli definiti dall'organizzazione]; [Assegnazione: elementi definiti dall'organizzazione all'interno dell'organizzazione]; [Assegnazione: organizzazioni esterne definite dall'organizzazione]]; e d. Implementa le direttive di sicurezza	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	secondo le tempistic he stabilite o notifica all'organizzazione emittente il grado di non conformità. Guida supplemen tare: lo United States Computer Emergency Readiness Team (US-CERT) genera avvisi e consigli di sicurezza per mantenere la consapevolezza della situazione in tutto il governo federale. Le direttive di sicurezza sono emesse dall'OMB o da altre organizza zioni designate con la responsab ilità e l'autorità di emettere tali direttive . La conformità alle direttive di sicurezza è essenziale a causa della natura critica di molte di esse e dei potenziali effetti negativi immediati sulle operazioni e sui beni dell'orga nizzazione, sulle persone, sulle altre		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	organizzazioni e sulla Nazione, qualora le direttive non vengano implementate in modo tempestivo. Le organizzazioni esterne comprendo no, ad esempio, partner esterni di missione/azienda, partner della catena di fornitura, fornitori di servizi esterni e altre organizzazioni di pari livello/supporto. Controllo correlato : SI-2. Riferimen ti: Pubblicazione speciale NIST 800-40.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-5	L'organizzazione: a. Riceve costantemente avvisi, consigli e direttive sulla sicurezza dei sistemi informativi da [Assegnazione: organizzazioni esterne definite dall'organizzazione]; b. Genera avvisi, consigli e direttive di sicurezza interna, se ritenuto necessario; c. Diffonde avvisi, consigli e direttive di sicurezza a: [Selezione (una o più): [Assegnazione: personale o ruoli definiti dall'organizzazione]; [Assegnazione: elementi definiti dall'organizzazione all'interno dell'organizzazione]; [Assegnazione: organizzazioni esterne definite dall'organizzazione]]; e d. Implementa le direttive di sicurezza	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	secondo le tempistic he stabilite o notifica all'organizzazione emittente il grado di non conformità. Guida supplemen tare: lo United States Computer Emergency Readiness Team (US-CERT) genera avvisi e consigli di sicurezza per mantenere la consapevolezza della situazione in tutto il governo federale. Le direttive di sicurezza sono emesse dall'OMB o da altre organizza zioni designate con la responsab ilità e l'autorità di emettere tali direttive . La conformità alle direttive di sicurezza è essenziale a causa della natura critica di molte di esse e dei potenziali effetti negativi immediati sulle operazioni e sui beni dell'orga nizzazione, sulle persone, sulle altre		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	organizzazioni e sulla Nazione, qualora le direttive non vengano implementate in modo tempestivo. Le organizzazioni esterne comprendo no, ad esempio, partner esterni di missione/azienda, partner della catena di fornitura, fornitori di servizi esterni e altre organizzazioni di pari livello/supporto. Controllo correlato : SI-2. Riferimen ti: Pubblicazione speciale NIST 800-40.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-5	L'organizzazione: a. Riceve costantemente avvisi, consigli e direttive sulla sicurezza dei sistemi informativi da [Assegnazione: organizzazioni esterne definite dall'organizzazione]; b. Genera avvisi, consigli e direttive di sicurezza interna, se ritenuto necessario; c. Diffonde avvisi, consigli e direttive di sicurezza a: [Selezione (una o più): [Assegnazione: personale o ruoli definiti dall'organizzazione]; [Assegnazione: elementi definiti dall'organizzazione all'interno dell'organizzazione]; [Assegnazione: organizzazioni esterne definite dall'organizzazione]]; e d. Implementa le direttive di sicurezza	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	secondo le tempistic he stabilite o notifica all'organizzazione emittente il grado di non conformità. Guida supplemen tare: lo United States Computer Emergency Readiness Team (US-CERT) genera avvisi e consigli di sicurezza per mantenere la consapevolezza della situazione in tutto il governo federale. Le direttive di sicurezza sono emesse dall'OMB o da altre organizza zioni designate con la responsab ilità e l'autorità di emettere tali direttive . La conformità alle direttive di sicurezza è essenziale a causa della natura critica di molte di esse e dei potenziali effetti negativi immediati sulle operazioni e sui beni dell'orga nizzazione, sulle persone, sulle altre		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	organizzazioni e sulla Nazione, qualora le direttive non vengano implementate in modo tempestivo. Le organizzazioni esterne comprendo no, ad esempio, partner esterni di missione/azienda, partner della catena di fornitura, fornitori di servizi esterni e altre organizzazioni di pari livello/supporto. Controllo correlato : SI-2. Riferimen ti: Pubblicazione speciale NIST 800-40.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(1)	Il sistema informativo esegue un controllo di integrità degli eventi rilevanti per la sicurezza almeno una volta al mese.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(1)	Il sistema informativo esegue un controllo di integrità degli eventi rilevanti per la sicurezza almeno una volta al mese.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(1)	Il sistema informativo esegue un controllo di integrità degli eventi rilevanti per la sicurezza almeno una volta al mese.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7	L'organizzazione utilizza strumenti di verifica dell'integrità per rilevare modifiche non autorizzate a [Assegnazione: software, firmware e informazioni definiti dall'organizzazione].	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-11	Il sistema informativo: a. Genera messaggi di errore che forniscono le informazioni necessarie per le azioni correttive senza rivelare informazioni che potrebbero essere sfruttate dagli avversari; e b. Rivela i messaggi di errore solo a [Assegnazione: personale o ruoli definiti dall'organizzazione]. Guida supplementare: le organizzazioni considerano attentamente la struttura/il contenuto dei messaggi di errore. La misura in cui i sistemi informativi sono in grado di identificare e gestire le condizioni di errore è guidata dalla policy dell'organizzazione e dai requisiti operativi. Le informazioni che potrebbero essere sfruttate dagli avversari includono,	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ad esempio, tentativi di accesso errati con password inserite per errore come nome utente, informazi oni su missioni/ aziende che possono essere ricavate da (se non esplicita mente dichiarate da) informazioni registrate e informazi oni personali come numeri di conto, numeri di previdenz a sociale e numeri di carte di credito. Inoltre, i messaggi di errore possono fornire un canale nascosto per la trasmissione di informazioni. Controlli correlati: AU-2, AU-3, SC-31. Miglioramenti di controllo: nessuno. Riferimenti: nessuno.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-11	Il sistema informativo: a. Genera messaggi di errore che forniscono le informazioni necessarie per le azioni correttive senza rivelare informazioni che potrebbero essere sfruttate dagli avversari; e b. Rivela i messaggi di errore solo a [Assegnazione: personale o ruoli definiti dall'organizzazione]. Guida supplementare: le organizzazioni considerano attentamente la struttura/il contenuto dei messaggi di errore. La misura in cui i sistemi informativi sono in grado di identificare e gestire le condizioni di errore è guidata dalla policy dell'organizzazione e dai requisiti operativi. Le informazioni che potrebbero essere sfruttate dagli avversari includono,	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ad esempio, tentativi di accesso errati con password inserite per errore come nome utente, informazi oni su missioni/ aziende che possono essere ricavate da (se non esplicita mente dichiarate da) informazioni registrate e informazi oni personali come numeri di conto, numeri di previdenz a sociale e numeri di carte di credito. Inoltre, i messaggi di errore possono fornire un canale nascosto per la trasmissione di informazioni. Controlli correlati: AU-2, AU-3, SC-31. Miglioramenti di controllo: nessuno. Riferimenti: nessuno.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-11	Il sistema informativo: a. Genera messaggi di errore che forniscono le informazioni necessarie per le azioni correttive senza rivelare informazioni che potrebbero essere sfruttate dagli avversari; e b. Rivela i messaggi di errore solo a [Assegnazione: personale o ruoli definiti dall'organizzazione]. Guida supplementare: le organizzazioni considerano attentamente la struttura/il contenuto dei messaggi di errore. La misura in cui i sistemi informativi sono in grado di identificare e gestire le condizioni di errore è guidata dalla policy dell'organizzazione e dai requisiti operativi. Le informazioni che potrebbero essere sfruttate dagli avversari includono,	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ad esempio, tentativi di accesso errati con password inserite per errore come nome utente, informazi oni su missioni/ aziende che possono essere ricavate da (se non esplicita mente dichiarate da) informazioni registrate e informazi oni personali come numeri di conto, numeri di previdenz a sociale e numeri di carte di credito. Inoltre, i messaggi di errore possono fornire un canale nascosto per la trasmissione di informazioni. Controlli correlati: AU-2, AU-3, SC-31. Miglioramenti di controllo: nessuno. Riferimenti: nessuno.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-11	Il sistema informativo: a. Genera messaggi di errore che forniscono le informazioni necessarie per le azioni correttive senza rivelare informazioni che potrebbero essere sfruttate dagli avversari; e b. Rivela i messaggi di errore solo a [Assegnazione: personale o ruoli definiti dall'organizzazione]. Guida supplementare: le organizzazioni considerano attentamente la struttura/il contenuto dei messaggi di errore. La misura in cui i sistemi informativi sono in grado di identificare e gestire le condizioni di errore è guidata dalla policy dell'organizzazione e dai requisiti operativi. Le informazioni che potrebbero essere sfruttate dagli avversari includono,	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ad esempio, tentativi di accesso errati con password inserite per errore come nome utente, informazi oni su missioni/ aziende che possono essere ricavate da (se non esplicita mente dichiarate da) informazioni registrate e informazi oni personali come numeri di conto, numeri di previdenz a sociale e numeri di carte di credito. Inoltre, i messaggi di errore possono fornire un canale nascosto per la trasmissione di informazioni. Controlli correlati: AU-2, AU-3, SC-31. Miglioramenti di controllo: nessuno. Riferimenti: nessuno.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-11	Il sistema informativo: a. Genera messaggi di errore che forniscono le informazioni necessarie per le azioni correttive senza rivelare informazioni che potrebbero essere sfruttate dagli avversari; e b. Rivela i messaggi di errore solo a [Assegnazione: personale o ruoli definiti dall'organizzazione]. Guida supplementare: le organizzazioni considerano attentamente la struttura/il contenuto dei messaggi di errore. La misura in cui i sistemi informativi sono in grado di identificare e gestire le condizioni di errore è guidata dalla policy dell'organizzazione e dai requisiti operativi. Le informazioni che potrebbero essere sfruttate dagli avversari includono,	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ad esempio, tentativi di accesso errati con password inserite per errore come nome utente, informazi oni su missioni/ aziende che possono essere ricavate da (se non esplicita mente dichiarate da) informazioni registrate e informazi oni personali come numeri di conto, numeri di previdenz a sociale e numeri di carte di credito. Inoltre, i messaggi di errore possono fornire un canale nascosto per la trasmissione di informazioni. Controlli correlati: AU-2, AU-3, SC-31. Miglioramenti di controllo: nessuno. Riferimenti: nessuno.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-11	Il sistema informativo: a. Genera messaggi di errore che forniscono le informazioni necessarie per le azioni correttive senza rivelare informazioni che potrebbero essere sfruttate dagli avversari; e b. Rivela i messaggi di errore solo a [Assegnazione: personale o ruoli definiti dall'organizzazione]. Guida supplementare: le organizzazioni considerano attentamente la struttura/il contenuto dei messaggi di errore. La misura in cui i sistemi informativi sono in grado di identificare e gestire le condizioni di errore è guidata dalla policy dell'organizzazione e dai requisiti operativi. Le informazioni che potrebbero essere sfruttate dagli avversari includono,	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ad esempio, tentativi di accesso errati con password inserite per errore come nome utente, informazi oni su missioni/ aziende che possono essere ricavate da (se non esplicita mente dichiarate da) informazioni registrate e informazi oni personali come numeri di conto, numeri di previdenz a sociale e numeri di carte di credito. Inoltre, i messaggi di errore possono fornire un canale nascosto per la trasmissione di informazioni. Controlli correlati: AU-2, AU-3, SC-31. Miglioramenti di controllo: nessuno. Riferimenti: nessuno.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-11	Il sistema informativo: a. Genera messaggi di errore che forniscono le informazioni necessarie per le azioni correttive senza rivelare informazioni che potrebbero essere sfruttate dagli avversari; e b. Rivela i messaggi di errore solo a [Assegnazione: personale o ruoli definiti dall'organizzazione]. Guida supplementare: le organizzazioni considerano attentamente la struttura/il contenuto dei messaggi di errore. La misura in cui i sistemi informativi sono in grado di identificare e gestire le condizioni di errore è guidata dalla policy dell'organizzazione e dai requisiti operativi. Le informazioni che potrebbero essere sfruttate dagli avversari includono,	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ad esempio, tentativi di accesso errati con password inserite per errore come nome utente, informazi oni su missioni/ aziende che possono essere ricavate da (se non esplicita mente dichiarate da) informazioni registrate e informazi oni personali come numeri di conto, numeri di previdenz a sociale e numeri di carte di credito. Inoltre, i messaggi di errore possono fornire un canale nascosto per la trasmissione di informazioni. Controlli correlati: AU-2, AU-3, SC-31. Miglioramenti di controllo: nessuno. Riferimenti: nessuno.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
SI-12	L'organizzazione gestisce e mantiene le informazioni all'inter no del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi , alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	cw-loggroup-retent ion-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzio ne dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruz ione e l'identificazione di eventi potenzial mente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-16	Il sistema informativo implementa [Assegnazione: misure di sicurezza definite dall'organizzazione] per proteggere la memoria dall'esecuzione di codice non autorizzato. Guida supplementare: alcuni avversari lanciano attacchi con l'intento di eseguire codice in regioni di memoria non eseguibili o in posizioni di memoria vietate. Le misure di sicurezza impiegate per proteggere la memoria includono, ad esempio, la prevenzione dell'esecuzione dei dati e la randomizzazione del layout dello spazio degli indirizzi. Le misure di protezione per la prevenzione dell'esecuzione dei dati possono essere applicate tramite hardware o software,	ecs-task-definition-memory-hard-limit	La limitazione della memoria massima disponibile per i container Amazon Elastic Container Service (ECS) garantisce che l'utilizzo delle risorse non possa essere abusato in caso di accesso malevolo ai container.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	con l'hardware che fornisce una maggiore robustezza del meccanismo. Controlli correlati: AC-25, SC-3. Miglioramenti di controllo: nessuno. Riferimenti: nessuno.		

Modello

Il modello è disponibile su GitHub: Operational Best Practices for FedRAMP (Moderate).

Best practice operative per FFIEC

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra i domini del Cyber Security Assessment Tool del Federal Financial Institutions Examination Council (FFIEC) e AWS le regole Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli FFIEC Cyber Security Assessment Tool. Un controllo FFIEC Cyber Security Assessment Tool può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.G.IT.B.1	Viene mantenuto un inventario delle risorse organizza	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	tive (ad esempio hardware, software, dati e sistemi ospitati esternamente).		all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.G.IT.B.1	Viene mantenuto un inventario delle risorse organizza tive (ad esempio hardware, software, dati e sistemi ospitati esternamente).	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.G.IT.B.1	Viene mantenuto un inventario delle risorse organizzative (ad esempio hardware, software, dati e sistemi ospitati esternamente).	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.G.IT.B.1	Viene mantenuto un inventario delle risorse organizza tive (ad esempio hardware, software, dati e sistemi ospitati esternamente).	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.Rm.B.1	All'interno dell'ente esiste una funzione di gestione del rischio per la sicurezza delle informazioni e la continuità operativa.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.RM.RA.B.2	La valutazione del rischio identifica i sistemi basati su Internet e le transazioni ad alto rischio che richiedono controlli di autenticazione aggiuntivi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
D1.RM.RA.B.2	La valutazione del rischio identifica i sistemi basati su Internet e le transazioni ad alto rischio che richiedono controlli di autenticazione aggiuntivi.	annual-risk-assessment-performed (controllo del processo)	Esegui una valutazione annuale del rischio sulla tua organizzazione. Le valutazioni del rischio possono aiutare a determinare la probabilità e l'impatto dei rischi e/o delle vulnerabilità identificati che interessano un'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.TC.Tr.B.2	La formazione annuale sulla sicurezza delle informazioni include la risposta agli incidenti, le minacce informatiche attuali (ad esempio phishing, spear phishing, ingegneria sociale e sicurezza mobile) e i problemi emergenti.	security-awareness-program-exists (controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.
D2.is.B.1	Le minacce alla sicurezza delle informazioni vengono raccolte e condivise con i dipendenti interni competenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.is.B.1	Le minacce alla sicurezza delle informazioni vengono raccolte e condivise con i dipendenti interni competenti.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.is.B.1	Le minacce alla sicurezza delle informazioni vengono raccolte e condivise con i dipendenti interni competenti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	cw-loggroup-retent ion-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzio ne dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruz ione e l'identificazione di eventi potenzial mente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
D2.MA.Ma.B.1	I record dei registri di controllo e gli altri log degli eventi di sicurezza vengono esaminati e conservati in modo sicuro.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearc h di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservaz ione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibi lità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.2	I registri degli eventi informatici vengono utilizzati per le indagini dopo che si è verificato un evento.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
D2.MA.Ma.B.2	I registri degli eventi informatici vengono utilizzati per le indagini dopo che si è verificato un evento.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.2	I registri degli eventi informatici vengono utilizzati per le indagini dopo che si è verificato un evento.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.2	I registri degli eventi informatici vengono utilizzati per le indagini dopo che si è verificato un evento.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.2	I registri degli eventi informatici vengono utilizzati per le indagini dopo che si è verificato un evento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.2	I registri degli eventi informatici vengono utilizzati per le indagini dopo che si è verificato un evento.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.2	I registri degli eventi informatici vengono utilizzati per le indagini dopo che si è verificato un evento.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
D2.MA.Ma.B.2	I registri degli eventi informatici vengono utilizzati per le indagini dopo che si è verificato un evento.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.2	I registri degli eventi informatici vengono utilizzati per le indagini dopo che si è verificato un evento.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.MA.Ma.B.2	I registri degli eventi informatici vengono utilizzati per le indagini dopo che si è verificato un evento.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.TI.Ti.B.1	L'istituto appartiene o è abbonato a una o più fonti di condivisi one delle informazi oni su minacce e vulnerabilità che forniscono informazi oni sulle minacce (ad esempio, FS-ISAC, US-CERT).	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.TI.Ti.B.1	L'istituto appartiene o si abbona a una o più fonti di condivisione delle informazioni su minacce e vulnerabi lità che forniscono informazioni sulle minacce (ad esempio, FS-ISAC, US-CERT).	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.TI.Ti.B.2	Le informazioni sulle minacce vengono utilizzate per monitorare minacce e vulnerabilità.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.TI.Ti.B.2	Le informazioni sulle minacce vengono utilizzate per monitorare minacce e vulnerabilità.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.TI.Ti.B.2	Le informazioni sulle minacce vengono utilizzate per monitorare minacce e vulnerabilità.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.TI.Ti.B.2	Le informazioni sulle minacce vengono utilizzate per migliorar e la gestione e i controlli interni del rischio.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D2.TI.Ti.B.2	Le informazioni sulle minacce vengono utilizzate per migliorar e la gestione e i controlli interni del rischio.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.CC.PM.B.1	Viene implementato un programma di gestione delle patch che garantisce che le patch software e firmware vengano applicate tempestiv amente.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.CC.PM.B.1	Viene implementato un programma di gestione delle patch che garantisce che le patch software e firmware vengano applicate tempestiv amente.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.CC.PM.B.1	Viene implementato un programma di gestione delle patch che garantisce che le patch software e firmware vengano applicate tempestiv amente.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'install azione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relaziona le (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.CC.PM.B.1	Viene implementato un programma di gestione delle patch che garantisce che le patch software e firmware vengano applicate tempestiv amente.	redshift-cluster-m aintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizza zione. In particola re, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVers ionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltati vamente il preferred MaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotR etention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.CC.PM.B.1	I report sulla gestione delle patch vengono esaminati e riflettono le patch di sicurezza mancanti.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.CC.PM.B.1	I report sulla gestione delle patch vengono esaminati e riflettono le patch di sicurezza mancanti.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.CC.PM.B.1	I report sulla gestione delle patch vengono esaminati e riflettono le patch di sicurezza mancanti.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.CC.PM.B.1	I report sulla gestione delle patch vengono esaminati e riflettono le patch di sicurezza mancanti.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.1	L'istituto è in grado di rilevare attività anomale attraverso il monitoraggio in tutto l'ambiente.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.1	L'istituto è in grado di rilevare attività anomale attraverso il monitoraggio in tutto l'ambiente.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.1	L'istituto è in grado di rilevare attività anomale attraverso il monitoraggio in tutto l'ambiente.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.1	Le transazioni dei clienti che generano avvisi di attività anomale vengono monitorate e riviste.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.1	Le transazioni dei clienti che generano avvisi di attività anomale vengono monitorate e riviste.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.3	I log di accesso fisico e/o logico vengono esaminati in seguito agli eventi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.3	I log di accesso fisico e/o logico vengono esaminati in seguito agli eventi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.3	I log di accesso fisico e/o logico vengono esaminati in seguito agli eventi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.3	I log di accesso fisico e/o logico vengono esaminati in seguito agli eventi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.3	I log di accesso fisico e/o logico vengono esaminati in seguito agli eventi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.3	I log di accesso fisico e/o logico vengono esaminati in seguito agli eventi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
D3.DC.An.B.3	I log di accesso fisico e/o logico vengono esaminati in seguito agli eventi.	api-gw-execution-l ogging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.3	I log di accesso fisico e/o logico vengono esaminati in seguito agli eventi.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.3	I log di accesso fisico e/o logico vengono esaminati in seguito agli eventi.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
D3.DC.An.B.3	I log di accesso fisico e/o logico vengono esaminati in seguito agli eventi.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.3	I log di accesso fisico e/o logico vengono esaminati in seguito agli eventi.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.4	L'accesso ai sistemi critici da parte di terzi viene monitorato per rilevare eventuali attività non autorizzate o insolite	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.4	L'accesso ai sistemi critici da parte di terzi viene monitorato per rilevare eventuali attività non autorizza te o insolite	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.4	L'accesso ai sistemi critici da parte di terzi viene monitorato per rilevare eventuali attività non autorizzate o insolite	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.4	L'accesso ai sistemi critici da parte di terzi viene monitorato per rilevare eventuali attività non autorizzate o insolite	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.4	L'accesso ai sistemi critici da parte di terzi viene monitorato per rilevare eventuali attività non autorizzate o insolite	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
D3.DC.An.B.4	L'accesso ai sistemi critici da parte di terzi viene monitorato per rilevare eventuali attività non autorizzate o insolite	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.4	L'accesso ai sistemi critici da parte di terzi viene monitorato per rilevare eventuali attività non autorizza te o insolite	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
D3.DC.An.B.4	L'accesso ai sistemi critici da parte di terzi viene monitorato per rilevare eventuali attività non autorizza te o insolite	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.4	L'accesso ai sistemi critici da parte di terzi viene monitorato per rilevare eventuali attività non autorizza te o insolite	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.4	L'accesso ai sistemi critici da parte di terzi viene monitorato per rilevare eventuali attività non autorizzate o insolite	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.4	L'accesso ai sistemi critici da parte di terzi viene monitorato per rilevare eventuali attività non autorizzate o insolite	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
D3.DC.An.B.4	L'accesso ai sistemi critici da parte di terzi viene monitorato per rilevare eventuali attività non autorizzate o insolite	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.An.B.5	I privilegi elevati vengono monitorati.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registran do le azioni della Console di gestione e le chiamate API. AWS È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
D3.DC.An.B.5	I privilegi elevati vengono monitorati.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Ev.B.1	Viene stabilita una normale linea di base per l'attività di rete.	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.
D3.DC.Ev.B.1	Viene stabilita una normale linea di base per l'attività di rete.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Ev.B.1	Viene stabilita una normale linea di base per l'attività di rete.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
D3.DC.Ev.B.1	Viene stabilita una normale linea di base per l'attività di rete.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Ev.B.1	Viene stabilita una normale linea di base per l'attività di rete.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
D3.DC.Ev.B.1	Viene stabilita una normale linea di base per l'attività di rete.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Ev.B.1	Viene stabilita una normale linea di base per l'attività di rete.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Ev.B.1	Viene stabilita una normale linea di base per l'attività di rete.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Ev.B.1	Viene stabilita una normale linea di base per l'attività di rete.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Ev.B.2	Esistono meccanismi (ad esempio, avvisi antivirus, avvisi di eventi di registro) per avvisare la gestione di potenziali attacchi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Ev.B.3	Sono in atto processi per monitorare la presenza di utenti, dispositivi, connessioni e software non autorizzati.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Ev.B.3	Sono in atto processi per monitorare la presenza di utenti, dispositivi, connessioni e software non autorizzati.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Ev.B.3	Sono in atto processi per monitorare la presenza di utenti, dispositivi, connessioni e software non autorizzati.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Ev.B.3	Sono in atto processi per monitorare la presenza di utenti, dispositivi, connessioni e software non autorizzati.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Th.B.1	I test indipendenti (inclusi i test di penetrazione e la scansione delle vulnerabilità) vengono condotti in base alla valutazione del rischio per i sistemi rivolti verso l'esterno e la rete interna.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Th.B.1	I test indipendenti (inclusi i test di penetrazione e la scansione delle vulnerabilità) vengono condotti in base alla valutazione del rischio per i sistemi rivolti verso l'esterno e la rete interna.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.DC.Th.B.1	I test indipendenti (inclusi i test di penetrazione e la scansione delle vulnerabilità) vengono condotti in base alla valutazione del rischio per i sistemi rivolti verso l'esterno e la rete interna.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.1	L'accesso dei dipendenti è garantito ai sistemi e ai dati riservati in base alle responsabilità lavorative e ai principi del privilegio minimo.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.1	L'accesso dei dipendenti è garantito ai sistemi e ai dati riservati in base alle responsabilità lavorative e ai principi del privilegio minimo.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.1	L'accesso dei dipendenti è garantito ai sistemi e ai dati riservati in base alle responsabilità lavorative e ai principi del privilegio minimo.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.1	L'accesso dei dipendenti è garantito ai sistemi e ai dati riservati in base alle responsabilità lavorative e ai principi del privilegio minimo.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
D3.PC.Am.B.1	L'accesso dei dipendenti è garantito ai sistemi e ai dati riservati in base alle responsabilità lavorative e ai principi del privilegio minimo.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.1	L'accesso dei dipendenti è garantito ai sistemi e ai dati riservati in base alle responsabilità lavorative e ai principi del privilegio minimo.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
D3.PC.Am.B.1	L'accesso dei dipendenti è garantito ai sistemi e ai dati riservati in base alle responsabilità lavorative e ai principi del privilegio minimo.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.1	L'accesso dei dipendenti è garantito ai sistemi e ai dati riservati in base alle responsabilità lavorative e ai principi del privilegio minimo.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.1	L'accesso dei dipendenti è garantito ai sistemi e ai dati riservati in base alle responsabilità lavorative e ai principi del privilegio minimo.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.1	L'accesso dei dipendenti è garantito ai sistemi e ai dati riservati in base alle responsabilità lavorative e ai principi del privilegio minimo.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
D3.PC.Am.B.1	L'accesso dei dipendenti è garantito ai sistemi e ai dati riservati in base alle responsabilità lavorative e ai principi del privilegio minimo.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.10	Gli ambienti di produzione e non di produzione sono segregati per impedire accessi non autorizzati o modifiche alle risorse informative. (*N/A se non esiste un ambiente di produzione presso l'istituto o presso una terza parte dell'ente.)	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.10	Gli ambienti di produzione e non di produzione sono segregati per impedire accessi non autorizzati o modifiche alle risorse informative. (*N/A se non esiste un ambiente di produzione presso l'istituto o presso una terza parte dell'ente.)	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.10	Gli ambienti di produzione e non di produzione sono segregati per impedire accessi non autorizzati o modifiche alle risorse informative. (*N/A se non esiste un ambiente di produzione presso l'istituto o presso una terza parte dell'ente.)	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.10	Gli ambienti di produzione e non di produzione sono segregati per impedire accessi non autorizzati o modifiche alle risorse informative. (*N/A se non esiste un ambiente di produzione presso l'istituto o presso una terza parte dell'ente.)	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
D3.PC.Am.B.12	Tutte le password sono crittografate durante l'archiviazione e il transito.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.13	I dati riservati vengono crittografati quando vengono trasmessi su reti pubbliche o non affidabili (ad esempio, Internet).	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
D3.PC.Am.B.13	I dati riservati vengono crittografati quando vengono trasmessi su reti pubbliche o non affidabili (ad esempio, Internet).	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.13	I dati riservati vengono crittografati quando vengono trasmessi su reti pubbliche o non attendibili (ad esempio Internet).	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
D3.PC.Am.B.13	I dati riservati vengono crittografati quando vengono trasmessi su reti pubbliche o non attendibili (ad esempio Internet).	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.13	I dati riservati vengono crittografati quando vengono trasmessi su reti pubbliche o non attendibili (ad esempio Internet).	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
D3.PC.Am.B.13	I dati riservati vengono crittografati quando vengono trasmessi su reti pubbliche o non attendibili (ad esempio Internet).	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.13	I dati riservati vengono crittografati quando vengono trasmessi su reti pubbliche o non attendibili (ad esempio Internet).	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
D3.PC.Am.B.15	L'accesso remoto ai sistemi critici da parte di dipendenti, collaboratori e terze parti utilizza connessioni crittografate e autenticazione a più fattori.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.15	L'accesso remoto ai sistemi critici da parte di dipendenti, collaboratori e terze parti utilizza connessioni crittografate e autenticazione a più fattori.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.15	L'accesso remoto ai sistemi critici da parte di dipendenti, collaboratori e terze parti utilizza connessioni crittografate e autenticazione a più fattori.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.15	L'accesso remoto ai sistemi critici da parte di dipendent i, collaboratori e terze parti utilizza connessioni crittogra fate e autenticazione a più fattori.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.15	L'accesso remoto ai sistemi critici da parte di dipendent i, collaboratori e terze parti utilizza connessioni crittogra fate e autenticazione a più fattori.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
D3.PC.Am.B.15	L'accesso remoto ai sistemi critici da parte di dipendent i, collaboratori e terze parti utilizza connessioni crittogra fate e autenticazione a più fattori.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.15	L'accesso remoto ai sistemi critici da parte di dipendent i, collaboratori e terze parti utilizza connessioni crittogra fate e autenticazione a più fattori.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.16	Sono in atto controlli amministrativi, fisici o tecnici per impedire agli utenti senza responsabilità amministrative di installare software non autorizzato.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.16	Sono in atto controlli amministrativi, fisici o tecnici per impedire agli utenti senza responsabilità amministrative di installare software non autorizzato.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.16	Sono in atto controlli amministrativi, fisici o tecnici per impedire agli utenti senza responsabilità amministrative di installare software non autorizzato.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
D3.PC.Am.B.16	Sono in atto controlli amministrativi, fisici o tecnici per impedire agli utenti senza responsabilità amministrative di installare software non autorizzato.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.2	L'accesso dei dipendenti ai sistemi e ai dati riservati prevede la separazione dei compiti.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.2	L'accesso dei dipendenti ai sistemi e ai dati riservati prevede la separazione dei compiti.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
D3.PC.Am.B.2	L'accesso dei dipendenti ai sistemi e ai dati riservati prevede la separazione dei compiti.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.3	I privilegi elevati (ad esempio i privilegi di amministratore) sono limitati e strettamente controllati (ad esempio, assegnati a singoli individui, non condivisi e richiedono controlli più rigorosi delle password)	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.3	I privilegi elevati (ad esempio i privilegi di amministratore) sono limitati e strettamente controllati (ad esempio, assegnati a singoli individui, non condivisi e richiedono controlli più rigorosi delle password)	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.3	I privilegi elevati (ad esempio i privilegi di amministratore) sono limitati e strettamente controllati (ad esempio, assegnati a singoli utenti, non condivisi e richiedono controlli più rigorosi delle password).	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.3	I privilegi elevati (ad esempio i privilegi di amministratore) sono limitati e strettamente controllati (ad esempio, assegnati a singoli individui, non condivisi e richiedono controlli più rigorosi delle password)	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.3	I privilegi elevati (ad esempio i privilegi di amministratore) sono limitati e strettamente controllati (ad esempio, assegnati a singoli utenti, non condivisi e richiedono controlli più rigorosi in materia di password)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.3	I privilegi elevati (ad esempio i privilegi di amministratore) sono limitati e strettamente controllati (ad esempio, assegnati a singoli individui, non condivisi e richiedono controlli più rigorosi delle password)	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.6	L'identificazione e l'autenticazione sono richieste e gestite per l'accesso a sistemi, applicazioni e hardware.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.6	L'identificazione e l'autenticazione sono richieste e gestite per l'accesso a sistemi, applicazioni e hardware.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.6	L'identificazione e l'autenticazione sono richieste e gestite per l'accesso a sistemi, applicazioni e hardware.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.6	L'identificazione e l'autenticazione sono richieste e gestite per l'accesso a sistemi, applicazioni e hardware.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.6	L'identificazione e l'autenticazione sono richieste e gestite per l'accesso a sistemi, applicazioni e hardware.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.6	L'identificazione e l'autenticazione sono richieste e gestite per l'accesso a sistemi, applicazioni e hardware.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.6	L'identificazione e l'autenticazione sono richieste e gestite per l'accesso a sistemi, applicazioni e hardware.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.6	L'identificazione e l'autenticazione sono richieste e gestite per l'accesso a sistemi, applicazioni e hardware.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.6	L'identificazione e l'autenticazione sono richieste e gestite per l'accesso a sistemi, applicazioni e hardware.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.6	L'identificazione e l'autenticazione sono richieste e gestite per l'accesso a sistemi, applicazioni e hardware.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
D3.PC.Am.B.6	L'identificazione e l'autenticazione sono richieste e gestite per l'accesso a sistemi, applicazioni e hardware.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.7	I controlli di accesso includono la complessità delle password e i limiti ai tentativi e al riutilizzo delle password.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Am.B.8	Tutte le password predefinite e gli account predefini ti non necessari vengono modificat i prima dell'impl ementazione del sistema.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio, router di frontiera e firewall).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio, router di frontiera e firewall).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio, router di frontiera e firewall).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale di rete (ad esempio router di frontiera e firewall).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale di rete (ad esempio router di frontiera e firewall).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale di rete (ad esempio router di frontiera e firewall).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale di rete (ad esempio router di frontiera e firewall).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio, router di frontiera e firewall).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	api-gw-associated-with-waf	AWS WAF consente di configurare una serie di regole (denominate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale di rete (ad esempio router di frontiera e firewall).	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale di rete (ad esempio router di frontiera e firewall).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale della rete (ad esempio router di frontiera e firewall).	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.1	Vengono utilizzati strumenti di difesa perimetrale di rete (ad esempio router di frontiera e firewall).	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.2	I sistemi a cui si accede da Internet o da parti esterne sono protetti da firewall o altri dispositivi simili.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.2	I sistemi a cui si accede da Internet o da parti esterne sono protetti da firewall o altri dispositivi simili.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.2	I sistemi a cui si accede da Internet o da parti esterne sono protetti da firewall o altri dispositivi simili.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.2	I sistemi a cui si accede da Internet o da parti esterne sono protetti da firewall o altri dispositivi simili.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.2	I sistemi a cui si accede da Internet o da parti esterne sono protetti da firewall o altri dispositivi simili.	api-gw-associated-with-waf	AWS WAF ti consente di configurare una serie di regole (chiamate lista di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili da te definite. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.2	I sistemi a cui si accede da Internet o da parti esterne sono protetti da firewall o altri dispositivi simili.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.3	Tutte le porte sono monitorate.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registran do le azioni della Console di gestione e le chiamate API. AWS È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
D3.PC.IM.B.3	Tutte le porte sono monitorate.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.3	Tutte le porte sono monitorate.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
D3.PC.IM.B.3	Tutte le porte sono monitorate.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.3	Tutte le porte sono monitorate.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.3	Tutte le porte sono monitorate.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.5	Le configurazioni dei sistemi (per server, desktop, router, ecc.) seguono gli standard del settore e vengono applicate	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.5	Le configurazioni dei sistemi (per server, desktop, router, ecc.) seguono gli standard del settore e vengono applicate	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.5	Le configurazioni dei sistemi (per server, desktop, router, ecc.) seguono gli standard del settore e vengono applicate	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.6	Porte, funzioni, protocolli e servizi sono vietati se non sono più necessari per scopi commerciali.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.6	Porte, funzioni, protocolli e servizi sono vietati se non sono più necessari per scopi commerciali.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.6	Porte, funzioni, protocolli e servizi sono vietati se non sono più necessari per scopi commerciali.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.IM.B.6	Porte, funzioni, protocolli e servizi sono vietati se non sono più necessari per scopi commerciali.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.7	L'accesso per apportare modifiche alle configurazioni dei sistemi (incluse macchine virtuali e hypervisor) è controllato e monitorato.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
D3.PC.Im.B.7	L'accesso per apportare modifiche alle configurazioni dei sistemi (incluse macchine virtuali e hypervisor) è controllato e monitorato.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.7	L'accesso per apportare modifiche alle configurazioni dei sistemi (incluse macchine virtuali e hypervisor) è controllato e monitorato.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.7	L'accesso per apportare modifiche alle configurazioni dei sistemi (incluse macchine virtuali e hypervisor) è controllato e monitorato.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.7	L'accesso per apportare modifiche alle configurazioni dei sistemi (incluse macchine virtuali e hypervisor) è controllato e monitorato.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di gestione e le chiamate API. AWS È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
D3.PC.Im.B.7	L'accesso per apportare modifiche alle configurazioni dei sistemi (incluse macchine virtuali e hypervisor) è controllato e monitorato.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Im.B.7	L'accesso per apportare modifiche alle configurazioni dei sistemi (incluse macchine virtuali e hypervisor) è controllato e monitorato.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
D3.PC.Se.B.1	Gli sviluppatori che lavorano per l'istituto seguono pratiche sicure di codifica dei programmi, come parte di un ciclo di vita di sviluppo del sistema (SDLC), che soddisfano gli standard del settore.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D3.PC.Se.B.1	Gli sviluppatori che lavorano per l'istitut o seguono pratiche sicure di codifica dei programmi, come parte di un ciclo di vita di sviluppo del sistema (SDLC), che soddisfano gli standard del settore.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D4.C.Co.B.2	L'istituto garantisce che le connessioni di terze parti siano autorizzate.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D4.C.Co.B.2	L'istituto garantisce che le connessioni di terze parti siano autorizzate.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D4.C.Co.B.2	L'istituto garantisce che le connessioni di terze parti siano autorizzate.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D4.C.Co.B.2	L'istituto garantisce che le connessioni di terze parti siano autorizzate.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.1	I parametri di avviso sono impostati per rilevare gli incidenti di sicurezza delle informazioni che richiedono azioni di mitigazione.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.1	I parametri di avviso sono impostati per rilevare gli incidenti di sicurezza delle informazioni che richiedono azioni di mitigazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.1	I parametri di avviso sono impostati per rilevare gli incidenti di sicurezza delle informazioni che richiedono azioni di mitigazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
D5.DR.De.B.2	I report sulle prestazio ni del sistema contengono informazi oni che possono essere utilizzate come indicatore di rischio per rilevare incidenti di sicurezza delle informazioni	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.2	I report sulle prestazioni del sistema contengono informazioni che possono essere utilizzate come indicatore di rischio per rilevare incidenti di sicurezza delle informazioni	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
D5.DR.De.B.3	Sono in atto strumenti e processi per rilevare, avvisare e attivare il programma di risposta agli incidenti.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registran do le azioni della Console di gestione e le chiamate API. AWS È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.3	Sono in atto strumenti e processi per rilevare, avvisare e attivare il programma di risposta agli incidenti.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
D5.DR.De.B.3	Sono in atto strumenti e processi per rilevare, avvisare e attivare il programma di risposta agli incidenti.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.3	Sono in atto strumenti e processi per rilevare, avvisare e attivare il programma di risposta agli incidenti.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.3	Sono in atto strumenti e processi per rilevare, avvisare e attivare il programma di risposta agli incidenti.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.3	Sono in atto strumenti e processi per rilevare, avvisare e attivare il programma di risposta agli incidenti.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.3	Sono in atto strumenti e processi per rilevare, avvisare e attivare il programma di risposta agli incidenti.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.3	Sono in atto strumenti e processi per rilevare, avvisare e attivare il programma di risposta agli incidenti.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.3	Sono in atto strumenti e processi per rilevare, avvisare e attivare il programma di risposta agli incidenti.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.3	Sono in atto strumenti e processi per rilevare, avvisare e attivare il programma di risposta agli incidenti.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.3	Sono in atto strumenti e processi per rilevare, avvisare e attivare il programma di risposta agli incidenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.DR.De.B.3	Sono in atto strumenti e processi per rilevare, avvisare e attivare il programma di risposta agli incidenti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.ER.Es.B.4	Gli incidenti vengono classificati, registrati e tracciati.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.
D5.ir.pl.B.1	L'istituto ha documentato come reagirà e risponderà agli incidenti informatici.	response-plan-exists-maintained (controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuit à operativa, ripristin o d'emergenza e backup dei dati.	backup-recovery-po int-minimum-retent ion-check	Per facilitare i processi di backup dei dati, assicurat i che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionD ays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D5.IR.PI.B.6	Per ripristinare l'operatività in seguito a un incidente, l'ente prevede di utilizzare programmi di continuità operativa, ripristino d'emergenza e backup dei dati.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for FFIEC.

Best practice operative per il Cloud Computing Compliance Criteria Catalog (C5) in Germania

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti

di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il Germany Cloud Compliance Criteria Catalog (C5) e le regole AWS Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli Germany C5. Un controllo C5 in Germania può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	AWS Regola di configurazione	Linea guida
COS-01	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
COS-01	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF

ID controllo	AWS Regola di configurazione	Linea guida
		per garantire la protezione da attacchi dannosi.
COS-01	waf-regional-rule-not-empty	Assicurati che il tuo AWS WAF abbia una regola che non sia vuota. Una regola senza condizioni può comportare un comportamento non intenzion ale.
COS-01	waf-regional-rulegroup-not-empty	Assicurati che il tuo AWS WAF abbia un gruppo di regole che non sia vuoto. Un gruppo di regole vuoto potrebbe causare un comportamento indesider ato.
COS-01	waf-regional-webacl-not-empty	Un ACL Web allegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.

ID controllo	AWS Regola di configurazione	Linea guida
COS-01	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
COS-03	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
COS-03	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
COS-03	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
COS-03	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
COS-03	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di configurazione	Linea guida
COS-03	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
COS-03	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di configurazione	Linea guida
COS-03	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.
COS-03	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
COS-03	lambda-function-public-acce ss-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di configurazione	Linea guida
COS-03	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di configurazione	Linea guida
COS-03	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
COS-03	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
COS-03	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
COS-03	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.
COS-03	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di configurazione	Linea guida
COS-03	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
COS-03	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
COS-03	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS
COS-03	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di configurazione	Linea guida
COS-03	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
COS-05	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
COS-05	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
COS-05	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
COS-05	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
COS-05	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
COS-05	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.
COS-05	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
COS-05	rds-snapshots-public-prohib ited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
COS-05	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
COS-05	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
COS-05	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
COS-05	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di configurazione	Linea guida
COS-05	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
CRY-02	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
CRY-02	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	AWS Regola di configurazione	Linea guida
CRY-02	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: SecurityPolicy ELB -TLS-1-2-2017-0. Il valore effettivo deve essere conforme alle policy dell'organizzazione.
CRY-02	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	AWS Regola di configurazione	Linea guida
CRY-02	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CRY-02	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CRY-02	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
CRY-02	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
CRY-02	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
CRY-03	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	AWS Regola di configurazione	Linea guida
CRY-03	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
CRY-03	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
CRY-03	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.
CRY-03	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
CRY-03	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
CRY-03	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
CRY-03	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
CRY-03	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
CRY-03	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
CRY-03	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
CRY-03	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di configurazione	Linea guida
CRY-03	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CRY-03	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.
CRY-03	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
CRY-03	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.
CRY-03	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
CRY-03	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
CRY-03	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
CRY-03	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
CRY-04	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.
DEV-07	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di configurazione	Linea guida
DEV-07	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.
DEV-07	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di configurazione	Linea guida
DEV-07	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
DEV-07	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	AWS Regola di configurazione	Linea guida
DEV-07	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
IDM-01	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
IDM-01	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
IDM-01	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
IDM-01	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
IDM-01	secretsmanager-rotation-ena bled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianifica zione regolare può abbreviar e il periodo di attività di un segreto e ridurre potenzial mente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
IDM-01	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibili tà che un'identità riceva o mantenga privilegi eccessivi.
IDM-01	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	ecs-containers-nonprivileged	Per facilitare l'impleme ntazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).
IDM-01	ecs-containers-readonly-acc ess	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizza zioni esplicite di lettura/s crittura.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.
IDM-01	efs-access-point-enforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.
IDM-01	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch

ID controllo	AWS Regola di configurazione	Linea guida
IDM-01	rds-instance-iam-authentication-enabled	Assicurati che l'autenticazione AWS Identity and Access Management (IAM) sia abilitata sulle istanze di Amazon Relational Database Service (Amazon RDS) per controllare l'accesso a sistemi e asset. In questo modo il traffico di rete da e verso il database viene crittografato utilizzando Secure Sockets Layer (SSL). Non devi archiviare le credenziali dell'utente nel database, perché l'autenticazione è gestita esternamente.
IDM-01	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanismi di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzare le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-03	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.
IDM-03	secretsmanager-secret-unused	Se in AWS Secrets Manager sono presenti credenziali inutilizzate, è necessario disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola consente di impostare un valore su unusedForDays (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-08	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
CRY-01	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
IDM-09	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
IDM-09	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
IDM-09	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
IDM-09	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
OPS-01	clb-multiple-az	Elastic Load Balancing (ELB) distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurati che ELB abbia registrato istanze da più zone di disponibilità.
OPS-01	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurati che ELB abbia registrato istanze da più zone di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-01	lambda-vpc-multi-az-check	Se la tua funzione AWS Lambda è configurata per la connessione a un cloud privato virtuale (VPC) nel tuo account, implementa la funzione AWS Lambda in almeno due zone di disponibilità diverse per assicurarti che sia disponibile per elaborare gli eventi in caso di interruzione del servizio in una singola zona.
OPS-01	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relational Database Service (Amazon RDS). Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-01	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-01	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
OPS-01	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-01	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCU Threshold Percentage (Config Default: 80) e AccountWCU Threshold Percentage (Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-02	clb-multiple-az	Elastic Load Balancing (ELB) distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurati che ELB abbia registrato istanze da più zone di disponibilità.
OPS-02	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-02	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individua re le possibili cause su cui indagare.
OPS-02	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurati che ELB abbia registrato istanze da più zone di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-02	lambda-vpc-multi-az-check	Se la tua funzione AWS Lambda è configurata per la connessione a un cloud privato virtuale (VPC) nel tuo account, implementa la funzione AWS Lambda in almeno due zone di disponibilità diverse per assicurarti che sia disponibile per elaborare gli eventi in caso di interruzione del servizio in una singola zona.
OPS-02	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relational Database Service (Amazon RDS). Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-02	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-02	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
OPS-02	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-02	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCU Threshold Percentage (Config Default: 80) e AccountWCU Threshold Percentage (Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-07	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-07	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfar e i requisiti di conformit à aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyV alue (Config default: 1), (requiredRetentionD ays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-07	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.
OPS-07	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
OPS-07	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) richiede almeno tre nodi di dati per un'elevata disponibilità e tolleranza ai guasti. L'implementazione di un dominio OpenSearch di servizio con almeno tre nodi di dati garantisce le operazioni del cluster in caso di guasto di un nodo.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-07	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.
OPS-07	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-07	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
OPS-07	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-07	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
OPS-07	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-07	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.
OPS-07	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-07	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
OPS-07	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-12	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.
OPS-12	s3-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-13	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
OPS-13	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-13	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di configurazione	Linea guida
OPS-14	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrai l Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
OPS-14	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail

ID controllo	AWS Regola di configurazione	Linea guida
OPS-14	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.
OPS-14	s3-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.
OPS-15	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-15	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
OPS-15	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.
OPS-15	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-15	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
OPS-15	opensearch-audit-logging-en abled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearc h Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-15	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
OPS-15	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
OPS-15	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-15	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
OPS-15	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-15	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'inter no dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
OPS-15	cloudtrail-enabled	AWS CloudTrail può contribui re a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-15	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
OPS-15	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-15	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di configurazione	Linea guida
OPS-22	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilitazione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.
PSS-05	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
PSS-05	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
PSS-05	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
PSS-05	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
PSS-07	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.

Modello

Il modello è disponibile su GitHub: Germany Cloud Compliance Criteria Catalog (C5).

Best practice operative per il Gramm Leach Bliley Act (GLBA)

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il Gramm-Leach-Bliley Act (GLBA) e le regole AWS Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli GLBA. Un controllo GLBA può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	alle salvaguardie amministrative, tecniche e fisiche		necessario il controllo degli accessi.
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	codebuild-project-s3-logs-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per AWS CodeBuild i log archiviati in Amazon S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(1)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (1) per assicurare e la sicurezza e la riservatezza dei registri e delle informazioni dei clienti;	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(2)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (2) per proteggere da qualsiasi minaccia o pericolo previsto per la sicurezza o l'integrità di tali registrazioni; e	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(2)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (2) per proteggere da qualsiasi minaccia o pericolo previsto per la sicurezza o l'integrità di tali registrazioni; e	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere e dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	efs-access-point-enforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
GLBA-SEC.501(b)(3)	Per favorire la policy di cui alla sottosezione (a), ogni agenzia o autorità descritta nella sezione 505(a) stabilirà standard appropriati per le istituzioni finanziarie soggette alla propria giurisdizione in merito alle salvaguardie amministrative, tecniche e fisiche (3) per proteggere dall'accesso non autorizzato o dall'uso di tali record o informazioni che potrebbero causare danni o disagi sostanziali a qualsiasi cliente.	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for Gramm Leach Bliley Act (GLBA).

Best practice operative per GxP dell'UE Allegato 11

I Conformance Pack forniscono un framework di conformità generico progettato per consentire all'utente di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena

conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra GxP EU Annex 11 e le regole AWS Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli GxP EU Annex 11. Un controllo GxP dell'UE Allegato 11 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1. Gestione del rischio	La gestione del rischio deve essere applicata durante l'intero ciclo di vita del sistema informati zzato, tenendo conto della sicurezza del paziente, dell'integrità dei dati e della qualità del prodotto. Nell'ambi to di un sistema di gestione del rischio, le decisioni sulla portata della convalida e dei controlli di integrità dei dati devono basarsi su una valutazione del rischio giustific ata e documentata del sistema informati zzato.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
1. Gestione del rischio	La gestione del rischio deve essere applicata durante l'intero ciclo di vita	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	del sistema informati zzato, tenendo conto della sicurezza del paziente, dell'integrità dei dati e della qualità del prodotto. Nell'ambi to di un sistema di gestione del rischio, le decisioni sulla portata della convalida e dei controlli di integrità dei dati devono basarsi su una valutazione del rischio giustific ata e documentata del sistema informati zzato.		software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.2. Convalida : controllo delle modifiche alla documentazione	La documentazione di convalida deve includere i record di controllo delle modifiche (se applicabile) e i report su eventuali deviazioni osservate durante il processo di convalida.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.3. Convalida: inventario	Deve essere disponibile un elenco aggiornato di tutti i sistemi pertinenti e della loro funzionalità GMP (inventario). Per i sistemi critici deve essere disponibile una descrizione aggiornata del sistema che descriva in dettaglio le disposizioni fisiche e logiche, i flussi di dati e le interfacce con altri sistemi o processi, eventuali prerequisiti hardware e software e le misure di sicurezza.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.3. Convalida: inventario	Deve essere disponibile un elenco aggiornato di tutti i sistemi pertinenti e della loro funzionalità GMP (inventario). Per i sistemi critici deve essere disponibile una descrizione aggiornata del sistema che descriva in dettaglio le disposizioni fisiche e logiche, i flussi di dati e le interfacce con altri sistemi o processi, eventuali prerequisiti hardware e software e le misure di sicurezza.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.3. Convalida: inventario	Deve essere disponibile un elenco aggiornato di tutti i sistemi pertinenti e della loro funzionalità GMP (inventario). Per i sistemi critici deve essere disponibile una descrizione aggiornata del sistema che descriva in dettaglio le disposizioni fisiche e logiche, i flussi di dati e le interfacce con altri sistemi o processi, eventuali prerequisiti hardware e software e le misure di sicurezza.	ec2-security-group-attached-to-eni-periodic	Per aiutarti a gestire il tuo inventario di asset, questa regola controlla se i gruppi di sicurezza sono collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a un'interfaccia di rete elastica. Se i tuoi gruppi di sicurezza non sono collegati a questi tipi di risorse, potrebbero essere inutilizzati e non più necessari.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.3. Convalida: inventario	Deve essere disponibile un elenco aggiornato di tutti i sistemi pertinenti e della loro funzionalità GMP (inventario). Per i sistemi critici deve essere disponibile una descrizione aggiornata del sistema che descriva in dettaglio le disposizioni fisiche e logiche, i flussi di dati e le interfacce con altri sistemi o processi, eventuali prerequisiti hardware e software e le misure di sicurezza.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.3. Convalida: inventario	Deve essere disponibile un elenco aggiornato di tutti i sistemi pertinenti e della loro funzionalità GMP (inventario). Per i sistemi critici deve essere disponibile una descrizione aggiornata del sistema che descriva in dettaglio le disposizioni fisiche e logiche, i flussi di dati e le interfacce con altri sistemi o processi, eventuali prerequisiti hardware e software e le misure di sicurezza.	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.3. Convalida: inventario	Deve essere disponibile un elenco aggiornato di tutti i sistemi pertinenti e della loro funzionalità GMP (inventario). Per i sistemi critici deve essere disponibile una descrizione aggiornata del sistema che descriva in dettaglio le disposizioni fisiche e logiche, i flussi di dati e le interfacce con altri sistemi o processi, eventuali prerequisiti hardware e software e le misure di sicurezza.	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazion e.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazion e.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazion e.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazion e.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.8. Convalida: trasferimento dei dati	Se i dati vengono trasferiti a un altro formato o sistema, la convalida deve includere controlli per verificare che tali dati non vengano alterati nel valore e/o nel significato durante il processo di migrazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Dati	I sistemi informatizzati che scambiano dati per via elettronica con altri sistemi devono prevedere adeguati controlli integrati per l'inserimento e l'elaborazione dei dati in modo corretto e sicuro, al fine di ridurre al minimo i rischi.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	dynamodb-pitr-enab led	Abilita questa regola per verificare che sia stato eseguito il backup delle informazi oni. Inoltre, mantiene i backup assicuran do che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristin o mantiene i backup continui della tabella degli ultimi 35 giorni.
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	dynamodb-table-enc rypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazi one predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettronici contro eventuali danni. È necessario verificare l'accessibilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettronici contro eventuali danni. È necessario verificare l'accessibilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	rds-snapshot-encry pted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	redshift-backup-en abled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatiz zati. Quando gli snapshot automatic i sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazi one predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	sagemaker-notebook -instance-kms-key- configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1. Archiviazione dei dati: protezione dai danni	I dati devono essere protetti sia con mezzi fisici che elettroni ci contro eventuali danni. È necessari o verificare l'accessi bilità, la leggibilità e l'accuratezza dei dati memorizzati. L'accesso ai dati deve essere garantito per tutto il periodo di conservazione.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accuratezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodicamente.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	backup-plan-min-fr equency-and-min-re tention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservaz ione minime. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredF requencyValue (Config default: 1), (requiredRetentionD aysConfig default: 35) e (requiredF requencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	backup-recovery-po int-minimum-retent ion-check	Per facilitare i processi di backup dei dati, assicurat i che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionD ays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accuratezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodicamente.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accuratezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodicamente.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	ebs-resources-prot ected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accuratezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodicamente.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accuratezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodicamente.	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accuratezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodicamente.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accuratezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodicamente.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2. Archiviazione dei dati: backup	È necessario eseguire backup regolari di tutti i dati pertinenti. L'integrità e l'accurat ezza dei dati di backup e la capacità di ripristinarli devono essere verificate durante la convalida e monitorate periodica mente.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9. Audit trail	Sulla base di una valutazione del rischio, è opportuno prendere in considera zione l'inserimento nel sistema di una registrazione di tutte le modifiche e le cancellazioni pertinenti alle GMP (una "audit trail" generata dal sistema). Per la modifica o la cancellazione dei dati pertinenti alle GMP, il motivo deve essere documentato. Le audit trail devono essere disponibili, convertibili in una forma generalmente comprensibile e riviste regolarmente.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10. Gestione delle modifiche e della configurazione	Qualsiasi modifica a un sistema informatizzato, comprese le configurazioni del sistema, deve essere effettuata solo in modo controllato e in conformità a una procedura definita.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10. Gestione delle modifiche e della configurazione	Qualsiasi modifica a un sistema informatizzato, comprese le configurazioni del sistema, deve essere effettuata solo in modo controllato e in conformità a una procedura definita.	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10. Gestione delle modifiche e della configurazione	Qualsiasi modifica a un sistema informati zzato, comprese le configurazioni del sistema, deve essere effettuata solo in modo controllato e in conformità a una procedura definita.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Valutazione periodica	I sistemi computerizzati devono essere valutati periodicamente per confermare che rimangano in uno stato valido e siano conformi alle GMP. Tali valutazioni devono includere, se necessario, l'attuale gamma di funzionalità, i record di deviazione, gli incidenti, i problemi, la cronologia degli aggiornamenti, le prestazioni, l'affidabilità, la sicurezza e i report sullo stato di convalida.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	codebuild-project-environment-privileged-check	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che il tuo ambiente di CodeBuild progetto Amazon non abbia la modalità privilegiata abilitata. Questa impostazione deve essere disabilitata per impedire l'accesso involontario alle API Docker e all'hardware sottostante del container.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	ecs-containers-nonprivileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	efs-access-point-enforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	rds-instance-iam-authentication-enabled	Assicurati che l'autenticazione AWS Identity and Access Management (IAM) sia abilitata sulle istanze di Amazon Relational Database Service (Amazon RDS) per controllare l'accesso a sistemi e asset. In questo modo il traffico di rete da e verso il database viene crittografato utilizzando Secure Sockets Layer (SSL). Non devi archiviare le credenziali dell'utente nel database, perché l'autenticazione è gestita esternamente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanismi di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzare le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.1. Sicurezza: persone autorizzate	È necessario predisporre controlli fisici e/o logici per limitare l'accesso al sistema informatico alle persone autorizzate. I metodi idonei per impedire l'accesso non autorizzato al sistema possono includere l'uso di chiavi, pass card, codici personali con password, biometria, accesso limitato alle apparecchiature informatiche e alle aree di archiviazione di dati.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.3. Sicurezza: audit trail autorizzazioni	La creazione, la modifica e l'annulla mento delle autorizza zioni di accesso devono essere registrati.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.4. Sicurezza: audit trail	I sistemi di gestione dei dati e dei documenti devono essere progettati per registrare l'identità degli operatori che inseriscono, modifican o, confermano o eliminano i dati, comprese data e ora.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12,4. Sicurezza: audit trail	I sistemi di gestione dei dati e dei documenti devono essere progettati per registrare l'identità degli operatori che inseriscono, modifican o, confermano o eliminano i dati, comprese data e ora.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.4. Sicurezza: audit trail	I sistemi di gestione dei dati e dei documenti devono essere progettati per registrare l'identità degli operatori che inseriscono, modifican o, confermano o eliminano i dati, comprese data e ora.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatc h Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazi oni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.4. Sicurezza: audit trail	I sistemi di gestione dei dati e dei documenti devono essere progettati per registrare l'identità degli operatori che inseriscono, modificano, confermano o eliminano i dati, comprese data e ora.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.4. Sicurezza: audit trail	I sistemi di gestione dei dati e dei documenti devono essere progettati per registrare l'identità degli operatori che inseriscono, modifican o, confermano o eliminano i dati, comprese data e ora.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.4. Sicurezza: audit trail	I sistemi di gestione dei dati e dei documenti devono essere progettati per registrare l'identità degli operatori che inseriscono, modificano, confermano o eliminano i dati, comprese data e ora.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.4. Sicurezza: audit trail	I sistemi di gestione dei dati e dei documenti devono essere progettati per registrare l'identità degli operatori che inseriscono, modificano, confermano o eliminano i dati, comprese data e ora.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
12.4. Sicurezza: audit trail	I sistemi di gestione dei dati e dei documenti devono essere progettati per registrare l'identità degli operatori che inseriscono, modificano, confermano o eliminano i dati, comprese data e ora.	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12,4. Sicurezza: audit trail	I sistemi di gestione dei dati e dei documenti devono essere progettati per registrare l'identità degli operatori che inseriscono, modifican o, confermano o eliminano i dati, comprese data e ora.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
12.4. Sicurezza: audit trail	I sistemi di gestione dei dati e dei documenti devono essere progettati per registrare l'identità degli operatori che inseriscono, modifican o, confermano o eliminano i dati, comprese data e ora.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12,4. Sicurezza: audit trail	I sistemi di gestione dei dati e dei documenti devono essere progettati per registrare l'identità degli operatori che inseriscono, modificano, confermano o eliminano i dati, comprese data e ora.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12.4. Sicurezza: audit trail	I sistemi di gestione dei dati e dei documenti devono essere progettati per registrare l'identità degli operatori che inseriscono, modifican o, confermano o eliminano i dati, comprese data e ora.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
13. Gestione degli incidenti	Segnala e valuta tutti gli incidenti, non solo i guasti del sistema e gli errori nei dati. La causa principale di un incidente critico deve essere identificata e deve costituire la base delle azioni correttive e preventive.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
13. Gestione degli incidenti	Segnala e valuta tutti gli incidenti, non solo i guasti del sistema e gli errori nei dati. La causa principale di un incidente critico deve essere identificata e deve costituire la base delle azioni correttive e preventive.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
16. Continuità aziendale	Per la disponibilità di sistemi computeri zzati che supportan o i processi critici, è necessario adottare disposizioni per garantire la continuit à del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizz o di sistemi alternati vi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportuna mente documentati e testati.	backup-recovery-po int-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per quanto riguarda la disponibilità di sistemi informatici a supporto dei processi critici, è opportuno adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per quanto riguarda la disponibilità di sistemi informatici a supporto dei processi critici, è opportuno adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati a supporto dei processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurati che ELB abbia registrato istanze da più zone di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per quanto riguarda la disponibilità di sistemi informatici a supporto dei processi critici, è opportuno adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per quanto riguarda la disponibilità di sistemi informatici a supporto dei processi critici, è opportuno adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	lambda-vpc-multi-az-check	Se la tua funzione AWS Lambda è configurata per la connessione a un cloud privato virtuale (VPC) nel tuo account, implementa la funzione AWS Lambda in almeno due zone di disponibilità diverse per assicurarti che sia disponibile per elaborare gli eventi in caso di interruzione del servizio in una singola zona.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi informatizzati a supporto dei processi critici, è opportuno adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) richiede almeno tre nodi di dati per un'elevata disponibilità e tolleranza ai guasti. L'implementazione di un dominio OpenSearch di servizio con almeno tre nodi di dati garantisce le operazioni del cluster in caso di guasto di un nodo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi informati ci a supporto dei processi critici, è necessario adottare disposizioni per garantire la continuit à del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizz o di sistemi alternati vi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportuna mente documentati e testati.	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per quanto riguarda la disponibilità di sistemi informatici a supporto dei processi critici, è opportuno adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per quanto riguarda la disponibilità di sistemi informatici a supporto dei processi critici, è opportuno adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati che supportano i processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per la disponibilità di sistemi computerizzati a supporto dei processi critici, è necessario adottare disposizioni per garantire la continuità del supporto di tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per quanto riguarda la disponibilità di sistemi informatici a supporto dei processi critici, è opportuno adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per quanto riguarda la disponibilità di sistemi informatici a supporto dei processi critici, è opportuno adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per quanto riguarda la disponibilità di sistemi informatici a supporto dei processi critici, è opportuno adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relational Database Service (Amazon RDS). Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
16. Continuità aziendale	Per quanto riguarda la disponibilità di sistemi informatici a supporto dei processi critici, è opportuno adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
16. Continuità aziendale	Per quanto riguarda la disponibilità di sistemi informatici a supporto dei processi critici, è opportuno adottare disposizioni per garantire la continuità del supporto a tali processi in caso di guasto del sistema (ad esempio un sistema manuale o alternativo). Il tempo necessario per l'utilizzo di sistemi alternativi deve essere basato sul rischio e adeguato a un particolare sistema e al processo aziendale che supporta. Questi accorgimenti devono essere opportunamente documentati e testati.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se si devono apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	aurora-resources-p rotected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	backup-plan-min-fr equency-and-min-re tention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservaz ione minime. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredF requencyValue (Config default: 1), (requiredRetentionD aysConfig default: 35) e (requiredF requencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	backup-recovery-po int-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se è necessario apportare modifiche rilevanti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificare l'accessibilità, la leggibilità e l'integrità di tali dati. Se è necessario apportare modifiche rilevanti al sistema (ad esempio apparecchiature o programmi informatici), è necessario garantire e testare la capacità di recuperare i dati.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se si devono apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	dynamodb-pitr-enab led	Abilita questa regola per verificare che sia stato eseguito il backup delle informazi oni. Inoltre, mantiene i backup assicuran do che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristin o mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificare l'accessibilità, la leggibilità e l'integrità di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informatici), è necessario garantire e testare la capacità di recuperare i dati.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificare l'accessibilità, la leggibilità e l'integrità di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informatici), è necessario garantire e testare la capacità di recuperare i dati.	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificare l'accessibilità, la leggibilità e l'integrità di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informatici), è necessario garantire e testare la capacità di recuperare i dati.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	efs-resources-prot ected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificare l'accessibilità, la leggibilità e l'integrità di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informatici), è necessario garantire e testare la capacità di recuperare i dati.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificare l'accessibilità, la leggibilità e l'integrità di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informatici), è necessario garantire e testare la capacità di recuperare i dati.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
17. Archiviazione	I dati possono essere archiviati. È necessario verificar e l'accessibilità, la leggibilità e l'integri tà di tali dati. Se è necessario apportare modifiche pertinenti al sistema (ad esempio apparecchiature o programmi informati ci), è necessario garantire e testare la capacità di recuperare i dati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for GxP EU Annex 11.

Best practice operative per la sicurezza HIPAA

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico

standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra l'Health Insurance Portability and Accountability Act (HIPAA) e le regole di Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli HIPAA. Un controllo HIPAA può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo Conformance Pack è stato convalidato da AWS Security Assurance Services LLC (AWS SAS), che è un team di Payment Card Industry Qualified Security Assessors (QSA), HITRUST Certified Common Security Framework Practitioners (ccSFP) e professionisti della conformità certificati per fornire indicazioni e valutazioni per vari framework di settore. AWS I professionisti SAS hanno progettato questo Conformance Pack per consentire a un cliente di allinearsi a un sottoinsieme dell'HIPAA.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(A)	(A) Analisi del rischio (obbligatoria). Effettua una valutazione accurata e approfondita dei potenziali rischi e vulnerabilità in materia di riservatezza, integrità e disponibilità delle informazioni sanitarie protette elettroniche detenute dall'entità interessata.	annual-risk-assessment-performed (Controllo del processo)	Esegui una valutazione annuale del rischio sulla tua organizzazione. Le valutazioni del rischio possono aiutare a determinare la probabilità e l'impatto dei rischi e/o delle vulnerabilità identificati che interessano un'organizzazione.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	e le vulnerabilità a un livello ragionevo le e appropriato conformemente alla Sezione 164.306(a).		le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficien ti a ridurre i rischi e le vulnerabilità a un livello ragionevo le e appropriato conformemente alla Sezione 164.306(a).	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(1)(ii)(B)	(B) Gestione del rischio (obbligatoria). Implementa misure di sicurezza sufficienti a ridurre i rischi e le vulnerabilità a un livello ragionevole e appropriato conformemente alla Sezione 164.306(a).	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroniche protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroniche protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanism i di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzar e le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(i)	(3)(i) Standard: sicurezza della forza lavoro. Implementa policy e procedure per garantire che tutti i membri della propria forza lavoro abbiano un accesso adeguato alle informazioni elettroni che protette sullo stato, come previsto dal paragrafo (a)(4) di questa sezione, e per evitare che i membri della forza lavoro che non hanno accesso ai sensi del paragrafo (a)(4) di questa sezione ottengano l'accesso alle informazioni elettroniche protette sullo stato.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearc h Service all'inter no di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(A)	(A) Autorizzazione e/o supervisione (indirizzabile). Implementare procedure per l'autorizzazione e/o la supervisione dei membri della forza lavoro che lavorano con informazioni elettroniche protette sullo stato o in luoghi in cui è possibile accedervi.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(B)	(B) Procedura di licenziamento del personale (indirizz abile). Implement are procedure per determinare che l'accesso di un membro della forza lavoro alle informazi oni elettroniche protette sullo stato sia appropriato.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
164.308(a)(3)(ii)(B)	(B) Procedura di licenziamento del personale (indirizz abile). Implement are procedure per determinare che l'accesso di un membro della forza lavoro alle informazi oni elettroniche protette sullo stato sia appropriato.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(B)	(B) Procedura di licenziamento del personale (indirizzabile). Implementare procedure per determinare che l'accesso di un membro della forza lavoro alle informazioni elettroniche protette sullo stato sia appropriato.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(B)	(B) Procedura di licenziamento del personale (indirizz abile). Implement are procedure per determinare che l'accesso di un membro della forza lavoro alle informazi oni elettroniche protette sullo stato sia appropriato.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
164.308(a)(3)(ii)(B)	(B) Procedura di licenziamento del personale (indirizz abile). Implement are procedure per determinare che l'accesso di un membro della forza lavoro alle informazi oni elettroniche protette sullo stato sia appropriato.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(B)	(B) Procedura di licenziamento del personale (indirizz abile). Implement are procedure per determinare che l'accesso di un membro della forza lavoro alle informazi oni elettroniche protette sullo stato sia appropriato.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(B)	(B) Procedura di licenziamento del personale (indirizz abile). Implement are procedure per determinare che l'accesso di un membro della forza lavoro alle informazi oni elettroniche protette sullo stato sia appropriato.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
164.308(a)(3)(ii)(B)	(B) Procedura di licenziamento del personale (indirizz abile). Implement are procedure per determinare che l'accesso di un membro della forza lavoro alle informazi oni elettroniche protette sullo stato sia appropriato.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(B)	(B) Procedura di licenziamento del personale (indirizzabile). Implementare procedure per determinare che l'accesso di un membro della forza lavoro alle informazioni elettroniche protette sullo stato sia appropriato.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(B)	(B) Procedura di licenziamento del personale (indirizz abile). Implement are procedure per determinare che l'accesso di un membro della forza lavoro alle informazi oni elettroniche protette sullo stato sia appropriato.	autoscaling-launch -config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(B)	(B) Procedura di licenziamento del personale (indirizzabile). Implementare procedure per determinare che l'accesso di un membro della forza lavoro alle informazioni elettroniche protette sullo stato sia appropriato.	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanismi di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzare le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(3)(ii)(C)	(C) Procedure di risoluzione (indirizz abili). Implement a procedure per interrompere l'accesso alle informazioni elettroni che protette sullo stato quando termina il rapporto di lavoro di un membro del personale o come richiesto dalle decisioni prese come specificato nel paragrafo (a)(3)(ii)(B) di questa sezione.	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizza tiva. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(i)	(4)(i) Standard: gestione dell'acce sso alle informazi oni. Implementare policy e procedure per autorizzare l'accesso alle informazioni elettroniche protette sullo stato che siano coerenti con i requisiti applicabili della sottoparte E di questa parte.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
164.308(a)(4)(i)	(4)(i) Standard: gestione dell'acce sso alle informazi oni. Implementare policy e procedure per autorizzare l'accesso alle informazioni elettroniche protette sullo stato che siano coerenti con i requisiti applicabili della sottoparte E di questa parte.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(i)	(4)(i) Standard: gestione dell'accesso alle informazioni. Implementare policy e procedure per autorizzare l'accesso alle informazioni elettroniche protette sullo stato che siano coerenti con i requisiti applicabili della sottoparte E di questa parte.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(i)	(4)(i) Standard: gestione dell'accesso alle informazioni. Implementare policy e procedure per autorizzare l'accesso alle informazioni elettroniche protette sullo stato che siano coerenti con i requisiti applicabili della sottoparte E di questa parte.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
164.308(a)(4)(i)	(4)(i) Standard: gestione dell'accesso alle informazioni. Implementare policy e procedure per autorizzare l'accesso alle informazioni elettroniche protette sullo stato che siano coerenti con i requisiti applicabili della sottoparte E di questa parte.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(i)	(4)(i) Standard: gestione dell'accesso alle informazioni. Implementare policy e procedure per autorizzare l'accesso alle informazioni elettroniche protette sullo stato che siano coerenti con i requisiti applicabili della sottoparte E di questa parte.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(i)	(4)(i) Standard: gestione dell'accesso alle informazioni. Implementare policy e procedure per autorizzare l'accesso alle informazioni elettroniche protette sullo stato che siano coerenti con i requisiti applicabili della sottoparte E di questa parte.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
164.308(a)(4)(i)	(4)(i) Standard: gestione dell'accesso alle informazioni. Implementare policy e procedure per autorizzare l'accesso alle informazioni elettroniche protette sullo stato che siano coerenti con i requisiti applicabili della sottoparte E di questa parte.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(i)	(4)(i) Standard: gestione dell'accesso alle informazioni. Implementare policy e procedure per autorizzare l'accesso alle informazioni elettroniche protette sullo stato che siano coerenti con i requisiti applicabili della sottoparte E di questa parte.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(i)	(4)(i) Standard: gestione dell'accesso alle informazioni. Implementare policy e procedure per autorizzare l'accesso alle informazioni elettroniche protette sullo stato che siano coerenti con i requisiti applicabili della sottoparte E di questa parte.	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanismi di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzare le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligat orio). Se un centro di clearing sanitario fa parte di un'organi zzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroni che da accessi non autorizzati da parte dell'organizzazione più grande.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanismi di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzare le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(A)	(A) Isolare le funzioni del centro di clearing sanitario (obbligatorio). Se un centro di clearing sanitario fa parte di un'organizzazione più grande, deve implementare policy e procedure che tutelino le proprie informazioni sanitarie protette elettroniche da accessi non autorizzati da parte dell'organizzazione più grande.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizz abile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attravers o l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizz abile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attravers o l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizz abile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attravers o l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(B)	(B) Autorizzazione all'accesso (indirizzabile). Implementa policy e procedure per la concessione dell'accesso alle informazioni sanitarie protette elettroniche, ad esempio attraverso l'accesso a una postazione di lavoro, una transazione, un programma, un processo o a un altro meccanismo.	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanismi di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzare le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanismi di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzare le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(4)(ii)(C)	(C) Istituzione e modifica dell'accesso (indirizzabile). Implementa policy e procedure che, sulla base delle policy di autorizzazione all'accesso dell'entità, stabiliscono, documentano, rivedono e modificano il diritto di accesso di un utente a una stazione di lavoro, un'operazione, un programma o un processo.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(5)(ii)(A)	(A) Promemoria di sicurezza (indirizz abili). Aggiornamenti di sicurezza periodici.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(5)(ii)(A)	(A) Promemoria di sicurezza (indirizz abili). Aggiornamenti di sicurezza periodici.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(5)(ii)(A)	(A) Promemoria di sicurezza (indirizzabili). Aggiornamenti di sicurezza periodici.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(5)(ii)(A)	(A) Promemoria di sicurezza (indirizz abili). Aggiornamenti di sicurezza periodici.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'install azione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relaziona le (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(5)(ii)(B)	(B) Protezione da software dannoso (indirizzabile). Procedure per la protezione, l'individuazione e la segnalazione di software dannoso.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(5)(ii)(B)	(B) Protezione da software dannoso (indirizzabile). Procedure per la protezione, l'individuazione e la segnalazione di software dannoso.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(5)(ii)(B)	(B) Protezione da software dannoso (indirizzabile). Procedure per la protezione, l'individ uazione e la segnalazi one di software dannoso.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(5)(ii)(C)	(C) Monitoraggio degli accessi (indirizzabile). Procedure per monitorare i tentativi di accesso e segnalare le discrepanze.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(5)(ii)(C)	(C) Monitoraggio degli accessi (indirizzabile). Procedure per monitorare i tentativi di accesso e segnalare le discrepanze.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(5)(ii)(C)	(C) Monitoraggio degli accessi (indirizzabile). Procedure per monitorare i tentativi di accesso e segnalare le discrepanze.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(5)(ii)(D)	(D) Gestione delle password (indirizzabile). Procedure per la creazione, la modifica e la salvaguardia delle password.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(6)(i)	(6)(i) Standard: procedure relative agli incidenti di sicurezza . Implementa policy e procedure per affrontare gli incidenti di sicurezza.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(6)(ii)	(ii) Specifiche di implementazione: risposta e segnalazione (obbligatorie). Identifica gli incidenti di sicurezza sospetti o noti e rispondi al riguardo; attenua, per quanto possibile, gli effetti dannosi degli incidenti di sicurezza noti all'entità interessata; documenta gli incidenti di sicurezza e i loro esiti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(i)	(7)(i) Standard: piano di emergenza. È necessario stabilire (e implementare, se necessario) policy e procedure per rispondere a un'emergenza o ad altri eventi (ad esempio, incendi, atti di vandalismo, guasti al sistema e disastri naturali) che danneggiano i sistemi che contengono informazioni sanitarie protette in formato elettronico.	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazion i che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(A)	(A) Piano di backup dei dati (richiesto). Stabilisci e implement a procedure per creare e conservar e copie esatte recuperabili di informazioni sanitarie elettroniche protette.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(A)	(A) Piano di backup dei dati (richiesto). Stabilisci e implement a procedure per creare e conservar e copie esatte recuperabili di informazioni sanitarie elettroniche protette.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(A)	(A) Piano di backup dei dati (richiesto). Stabilisci e implement a procedure per creare e conservar e copie esatte recuperabili di informazioni sanitarie elettroniche protette.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(A)	(A) Piano di backup dei dati (richiesto). Stabilisci e implement a procedure per creare e conservar e copie esatte recuperabili di informazioni sanitarie elettroniche protette.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(A)	(A) Piano di backup dei dati (richiesto). Stabilisci e implement a procedure per creare e conservar e copie esatte recuperabili di informazioni sanitarie elettroniche protette.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(A)	(A) Piano di backup dei dati (richiesto). Stabilisci e implement a procedure per creare e conservar e copie esatte recuperabili di informazioni sanitarie elettroniche protette.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(A)	(A) Piano di backup dei dati (richiesto). Stabilisci e implement a procedure per creare e conservar e copie esatte recuperabili di informazioni sanitarie elettroniche protette.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(A)	(A) Piano di backup dei dati (richiesto). Stabilisci e implement a procedure per creare e conservar e copie esatte recuperabili di informazioni sanitarie elettroniche protette.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatiz zati. Quando gli snapshot automatic i sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazi one predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(A)	(A) Piano di backup dei dati (richiesto). Stabilisci e implement a procedure per creare e conservar e copie esatte recuperabili di informazioni sanitarie elettroniche protette.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(A)	(A) Piano di backup dei dati (richiesto). Stabilisci e implement a procedure per creare e conservar e copie esatte recuperabili di informazioni sanitarie elettroniche protette.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(A)	(A) Piano di backup dei dati (richiesto). Stabilisci e implement a procedure per creare e conservar e copie esatte recuperabili di informazioni sanitarie elettroniche protette.	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazion i che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(A)	(A) Piano di backup dei dati (richiesto). Stabilisci e implement a procedure per creare e conservar e copie esatte recuperabili di informazioni sanitarie elettroniche protette.	redshift-cluster-m aintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizza zione. In particola re, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrad e Il valore predefini to è true. Inoltre, consente di impostare facoltativamente il preferredMaintenan ceWindow (l'impost azione predefinita è sab: 16:00 -sab: 16:30) e il automated SnapshotRetention periodo (l'impost azione predefinita è 1). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(B)	(B) Piano di ripristino di emergenza (richiesto). Stabilisci (e implementa se necessario) procedure per ripristinare qualsiasi perdita di dati.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(B)	(B) Piano di ripristino di emergenza (richiesto). Stabilisci (e implementa se necessario) procedure per ripristinare qualsiasi perdita di dati.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(B)	(B) Piano di ripristino di emergenza (richiesto). Stabilisci (e implementa se necessario) procedure per ripristinare qualsiasi perdita di dati.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(B)	(B) Piano di ripristino di emergenza (richiesto). Stabilisci (e implementa se necessario) procedure per ripristinare qualsiasi perdita di dati.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(B)	(B) Piano di ripristino di emergenza (richiesto). Stabilisci (e implementa se necessario) procedure per ripristinare qualsiasi perdita di dati.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(B)	(B) Piano di ripristino di emergenza (richiesto). Stabilisci (e implementa se necessario) procedure per ripristinare qualsiasi perdita di dati.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(B)	(B) Piano di ripristino di emergenza (richiesto). Stabilisci (e implementa se necessario) procedure per ripristinare qualsiasi perdita di dati.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(B)	(B) Piano di ripristino di emergenza (richiesto). Stabilisci (e implementa se necessario) procedure per ripristinare qualsiasi perdita di dati.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(B)	(B) Piano di ripristino di emergenza (richiesto). Stabilisci (e implementa se necessario) procedure per ripristinare qualsiasi perdita di dati.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(B)	(B) Piano di ripristino di emergenza (richiesto). Stabilisci (e implementa se necessario) procedure per ripristinare qualsiasi perdita di dati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(B)	(B) Piano di ripristino di emergenza (richiesto). Stabilisci (e implementa se necessario) procedure per ripristinare qualsiasi perdita di dati.	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(C)	(C) Piano operativo in modalità di emergenza (obbligatorio). Stabilisci (e implementa se necessario) procedure per consentire la continuazione dei processi aziendali critici per la protezione e della sicurezza delle informazioni sanitarie protette elettronicamente durante il funzionamento in modalità di emergenza.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(C)	(C) Piano operativo in modalità di emergenza (obbligatorio). Stabilisci (e implementa se necessario) procedure per consentire la continuazione dei processi aziendali critici per la protezione e della sicurezza delle informazioni sanitarie protette elettronicamente durante il funzionamento in modalità di emergenza.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(C)	(C) Piano operativo in modalità di emergenza (obbligatorio). Stabilisci (e implementa se necessario) procedure per consentire la continuazione dei processi aziendali critici per la protezione e della sicurezza delle informazioni sanitarie protette elettronicamente durante il funzionamento in modalità di emergenza.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(C)	(C) Piano operativo in modalità di emergenza (obbligatorio). Stabilisci (e implementa se necessario) procedure per consentire la continuazione dei processi aziendali critici per la protezione e della sicurezza delle informazioni sanitarie protette elettronicamente durante il funzionamento in modalità di emergenza.	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(7)(ii)(C)	(C) Piano operativo in modalità di emergenza (obbligatorio). Stabilisci (e implementa se necessario) procedure per consentire la continuazione dei processi aziendali critici per la protezione e della sicurezza delle informazioni sanitarie protette elettronicamente durante il funzionamento in modalità di emergenza.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
164.308(a)(7)(ii)(C)	(C) Piano operativo in modalità di emergenza (obbligatorio). Stabilisci (e implementa se necessario) procedure per consentire la continuazione dei processi aziendali critici per la protezione e della sicurezza delle informazioni sanitarie protette elettronicamente durante il funzionamento in modalità di emergenza.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(8)	(8) Standard: valutazione. Esegui una valutazione periodica tecnica e non tecnica che sia basata inizialmente sugli standard implementati ai sensi della presente norma e successivamente, in risposta a cambiamenti ambientali o operativi che influiscono sulla sicurezza delle informazioni sanitarie protette elettroniche, che stabilisca in che misura le policy e le procedure di sicurezza di un'entità soddisfino i requisiti della presente sottoparte.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.308(a)(8)	(8) Standard: valutazione. Esegui una valutazione periodica tecnica e non tecnica che sia basata inizialmente sugli standard implementati ai sensi della presente norma e successivamente, in risposta a cambiamenti ambientali o operativi che influiscono sulla sicurezza delle informazioni sanitarie protette elettroniche, che stabilisca in che misura le policy e le procedure di sicurezza di un'entità soddisfino i requisiti della presente sottoparte.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	iam-user-unused-cr edentials-check	AWS Identity and Access Managemen t (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controlla ndo le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizz ate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegi o minimo. Questa regola richiede di impostare un valore su maxCreden tialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicuran do che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicuran do che i nodi master del cluster Amazon EMR non siano accessibili pubblicam ente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consenton o l'accesso bidirezio nale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	lambda-function-pu blic-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	s3-account-level-p ublic-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltati vamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPubl icAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	s3-bucket-level-pu blic-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCES S_KEY_ID e AWS_SECRE T_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	ecs-containers-rea donly-access	L'abilitazione dell'acce sso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettar e il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificat o a meno che non disponga di autorizza zioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in 164.308(a)(4).	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanism i di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzar e le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(1)	(a)(1) Standard: controllo degli accessi. Implement a policy e procedure tecniche per i sistemi informatici elettroni ci che conservano informazioni sanitarie protette in modo da consentire l'accesso solo alle persone o ai programmi software a cui sono stati concessi i diritti di accesso come specificato in ¤ 164.308(a)(4).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearc h Service all'inter no di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(i)	(2) Specifiche di implementazione: (i) Identificazione utente univoca (richiesta). Assegna un nome e/o un numero univoci per identificare e tracciare l'identità dell'utente.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligatoria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligat oria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.
164.312(a)(2)(ii)	(ii) Procedura di accesso di emergenza (obbligat oria). Stabilisci (e implementa se richiesto) procedure per ottenere le informazioni sanitarie elettroniche protette necessarie durante un'emergenza.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implement a un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(a)(2)(iv)	(iv) Crittografia e decrittografia (indirizzabile). Implementa un meccanismo per crittografare e decrittografare le informazioni sanitarie elettroniche protette.	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissi one assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportar e. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficien ti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissi one effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltati vamente i parametri AccountRCU ThresholdPercentag e (Config Default: 80) e AccountWCU ThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanismi procedurali che registrino ed esaminino l'attività nei sistemi informatici che contengono o utilizzano informazioni sanitarie elettroniche protette.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorar e la disponibilità di Amazon RDS. Ciò fornisce una visibilit à dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archivi azione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositi vo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearc h di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservaz ione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibi lità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	s3-event-notifications-enabled	Le notifiche degli eventi di Amazon S3 possono notificar e al personale competente eventuali modifiche accidenta li o intenzionali agli oggetti del bucket. Gli avvisi includono: creazione di un nuovo oggetto, rimozione di oggetti, ripristino di oggetti, oggetti persi e replicati.
164.312(b)	(b) Standard: controlli di audit. Implementa hardware, software e/o meccanism i procedurali che registrino ed esaminino l'attività nei sistemi informati ci che contengono o utilizzano informazioni sanitarie elettroniche protette.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearc h di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearc h I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosti care problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(c)(1)	(c)(1) Standard: integrità. Implement a policy e procedure per salvaguardare le informazioni sanitarie elettroniche protette da alterazioni o distruzioni improprie.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(c)(1)	(c)(1) Standard: integrità. Implement a policy e procedure per salvaguardare le informazioni sanitarie elettroniche protette da alterazioni o distruzioni improprie.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(c)(1)	(c)(1) Standard: integrità. Implement a policy e procedure per salvaguardare le informazioni sanitarie elettroniche protette da alterazioni o distruzioni improprie.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei registri. CloudTrai l La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificar e, eliminare o falsifica re i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(c)(1)	(c)(1) Standard: integrità. Implement a policy e procedure per salvaguardare le informazioni sanitarie elettroniche protette da alterazioni o distruzioni improprie.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
164.312(c)(1)	(c)(1) Standard: integrità. Implement a policy e procedure per salvaguardare le informazioni sanitarie elettroniche protette da alterazioni o distruzioni improprie.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(c)(2)	(2) Specifiche di implementazione: meccanismo di autenticazione delle informazioni sanitarie protette elettroniche (indirizzabile). Implementa meccanismi elettronici per confermare che le informazioni sanitarie protette elettroni che non siano state alterate o distrutte in modo non autorizzato.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(c)(2)	(2) Specifiche di implementazione: meccanismo di autenticazione delle informazioni sanitarie protette elettroniche (indirizz abile). Implementa meccanismi elettronici per confermare che le informazioni sanitarie protette elettroni che non siano state alterate o distrutte in modo non autorizzato.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
164.312(c)(2)	(2) Specifiche di implementazione: meccanismo di autenticazione delle informazioni sanitarie protette elettroniche (indirizz abile). Implementa meccanismi elettronici per confermare che le informazioni sanitarie protette elettroni che non siano state alterate o distrutte in modo non autorizzato.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(c)(2)	(2) Specifiche di implementazione: meccanismo di autenticazione delle informazioni sanitarie protette elettroniche (indirizzabile). Implementa meccanismi elettronici per confermare che le informazioni sanitarie protette elettroni che non siano state alterate o distrutte in modo non autorizzato.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(c)(2)	(2) Specifiche di implementazione: meccanismo di autenticazione delle informazioni sanitarie protette elettroniche (indirizz abile). Implementa meccanismi elettronici per confermare che le informazioni sanitarie protette elettroni che non siano state alterate o distrutte in modo non autorizzato.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(d)	(d) Standard: autenticazione di persone o entità. Implement a procedure per verificare che la persona o l'entità che desidera accedere a informazioni sanitarie elettroniche protette sia quella dichiarata.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la AWS sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(d)	(d) Standard: autenticazione di persone o entità. Implement a procedure per verificare che la persona o l'entità che desidera accedere a informazioni sanitarie elettroniche protette sia quella dichiarata.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(d)	(d) Standard: autenticazione di persone o entità. Implement a procedure per verificare che la persona o l'entità che desidera accedere a informazioni sanitarie elettroniche protette sia quella dichiarata.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(d)	(d) Standard: autenticazione di persone o entità. Implement a procedure per verificare che la persona o l'entità che desidera accedere a informazioni sanitarie elettroniche protette sia quella dichiarata.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(d)	(d) Standard: autenticazione di persone o entità. Implement a procedure per verificare che la persona o l'entità che desidera accedere a informazioni sanitarie elettroniche protette sia quella dichiarata.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richieden do l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(1)	(e)(1) Standard: sicurezza della trasmissione. Implementa misure tecniche di sicurezza per prevenire l'accesso non autorizzato alle informazioni sanitarie elettroniche protette che vengono trasmesse su una rete di comunicazione elettronica.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(e)(2)(i)	(i) Controlli di integrità (indirizzabili). Implementa misure di sicurezza per garantire che le informazioni sanitarie elettroniche protette trasmesse elettronicamente non vengano modificate in modo improprio senza essere rilevate fino allo smaltimento.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(i)	(i) Controlli di integrità (indirizz abili). Implementa misure di sicurezza per garantire che le informazioni sanitarie elettroniche protette trasmesse elettroni camente non vengano modificate in modo improprio senza essere rilevate fino allo smaltimento.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
164.312(e)(2)(i)	(i) Controlli di integrità (indirizz abili). Implementa misure di sicurezza per garantire che le informazioni sanitarie elettroniche protette trasmesse elettroni camente non vengano modificate in modo improprio senza essere rilevate fino allo smaltimento.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(i)	(i) Controlli di integrità (indirizz abili). Implementa misure di sicurezza per garantire che le informazioni sanitarie elettroniche protette trasmesse elettroni camente non vengano modificate in modo improprio senza essere rilevate fino allo smaltimento.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(i)	(i) Controlli di integrità (indirizzabili). Implementa misure di sicurezza per garantire che le informazioni sanitarie elettroniche protette trasmesse elettronicamente non vengano modificate in modo improprio senza essere rilevate fino allo smaltimento.	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
164.312(e)(2)(i)	(i) Controlli di integrità (indirizzabili). Implementa misure di sicurezza per garantire che le informazioni sanitarie elettroniche protette trasmesse elettronicamente non vengano modificate in modo improprio senza essere rilevate fino allo smaltimento.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(e)(2)(i)	(i) Controlli di integrità (indirizzabili). Implementa misure di sicurezza per garantire che le informazioni sanitarie elettroniche protette trasmesse elettronicamente non vengano modificate in modo improprio senza essere rilevate fino allo smaltimento.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(i)	(i) Controlli di integrità (indirizz abili). Implementa misure di sicurezza per garantire che le informazioni sanitarie elettroniche protette trasmesse elettroni camente non vengano modificate in modo improprio senza essere rilevate fino allo smaltimento.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(e)(2)(i)	(i) Controlli di integrità (indirizz abili). Implementa misure di sicurezza per garantire che le informazioni sanitarie elettroniche protette trasmesse elettroni camente non vengano modificate in modo improprio senza essere rilevate fino allo smaltimento.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(i)	(i) Controlli di integrità (indirizzabili). Implementa misure di sicurezza per garantire che le informazioni sanitarie elettroniche protette trasmesse elettronicamente non vengano modificate in modo improprio senza essere rilevate fino allo smaltimento.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityP olicy Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
164.312(e)(2)(ii)	(ii) Crittografia (indirizzabile). Implementa un meccanismo di crittografia delle informazioni sanitarie elettroniche protette ogni qualvolta lo si ritenga opportuno.	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevole e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevole e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevole e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevole e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(1)	(b)(1) Standard: requisiti per i piani sanitari di gruppo. Ad eccezione dei casi in cui le uniche informazioni sanitarie protette elettroni che comunicate allo sponsor del piano sono comunicate ai sensi di 164.504(f)(1)(ii) o (iii), o come autorizzato ai sensi della norma¤164.508, un piano sanitario di gruppo deve garantire che i documenti del piano prevedano che lo sponsor del piano salvaguardi in modo ragionevo le e appropriato le informazioni sanitarie protette elettroniche create, ricevute, mantenute o trasmesse allo sponsor del piano o da quest'ultimo per conto del piano sanitario di gruppo.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo; (ii) garantire che l'adeguata separazione richiesta da 164.504(f)(2)(iii) sia supportata da misure di sicurezza ragionevoli e appropriate;	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(iii) garantire che qualsiasi agente, compresi i subappaltatori, a cui fornisce queste informazioni accetti di implementare misure di sicurezza ragionevoli e appropriate per proteggere le informazioni; e (iv) riferire al piano sanitario di gruppo qualsiasi incidente di sicurezza di cui venga a conoscenza.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanismi di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzare le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da AWS ACM. Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: ELB -TLS-1-2-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			2017-0. SecurityPolicy Il valore effettivo deve essere conforme alle policy dell'organizzazione.
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
164.314(b)(2)(i)	(2) Specifiche di implementazione (obbligatorie). I documenti del piano sanitario di gruppo devono essere modificati per incorporare disposizioni che richiedano allo sponsor del piano di - (i) implementare salvaguardie amministrative, fisiche e tecniche che proteggano in modo ragionevole e appropriato la riservatezza, l'integrità e la disponibilità delle informazioni sanitarie protette elettroniche create, ricevute, conservate o trasmesse per conto del piano sanitario di gruppo;	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for HIPAA Security.

Best practice operative per IRS 1075

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra l'IRS 1075 e le regole AWS Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli IRS 1075. Un controllo IRS 1075 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing d. Crittografia dei dati in transito	L'FTI deve essere crittografato durante il transito all'interno dell'ambiente cloud. Tutti i meccanismi utilizzati per crittografare l'FTI devono essere certificati FIPS 140 e funzionare utilizzando i più recenti moduli conformi a FIPS 140. Questo requisito deve essere incluso nello SLA.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.3.1 Cloud computing d. Crittografia dei dati in transito	L'FTI deve essere crittografato durante il transito all'interno dell'ambiente cloud. Tutti i meccanismi	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	utilizzati per crittografare l'FTI devono essere certificati FIPS 140 e funzionare utilizzando i più recenti moduli conformi a FIPS 140. Questo requisito deve essere incluso nello SLA.		node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.3.1 Cloud computing d. Crittografia dei dati in transito	L'FTI deve essere crittografato durante il transito all'interno dell'ambiente cloud. Tutti i meccanismi utilizzati per crittografare l'FTI devono essere certificati FIPS 140 e funzionare utilizzando i più recenti moduli conformi a FIPS 140. Questo requisito deve essere incluso nello SLA.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing d. Crittografia dei dati in transito	L'FTI deve essere crittografato durante il transito all'interno dell'ambiente cloud. Tutti i meccanismi utilizzati per crittografare l'FTI devono essere certificati FIPS 140 e funzionare utilizzando i più recenti moduli conformi a FIPS 140. Questo requisito deve essere incluso nello SLA.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing d. Crittografia dei dati in transito	L'FTI deve essere crittografato durante il transito all'interno dell'ambiente cloud. Tutti i meccanismi utilizzati per crittografare l'FTI devono essere certificati FIPS 140 e funzionare utilizzando i più recenti moduli conformi a FIPS 140. Questo requisito deve essere incluso nello SLA.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing d. Crittografia dei dati in transito	L'FTI deve essere crittografato durante il transito all'interno dell'ambiente cloud. Tutti i meccanismi utilizzati per crittografare l'FTI devono essere certificati FIPS 140 e funzionare utilizzando i più recenti moduli conformi a FIPS 140. Questo requisito deve essere incluso nello SLA.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.3.1 Cloud computing d. Crittografia dei dati in transito	L'FTI deve essere crittografato durante il transito all'interno dell'ambiente cloud. Tutti i meccanismi utilizzati per crittografare l'FTI devono essere certificati FIPS 140 e funzionare utilizzando i più recenti moduli conformi a FIPS 140. Questo requisito deve essere incluso nello SLA.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
3.3.1 Cloud computing e. Crittografia dei dati a riposo	Crittografia dei dati a riposo: l'FTI deve essere crittografato mentre è a riposo nel cloud utilizzando il più recente meccanismo di crittografia certificato FIPS 140. Questo requisito deve essere incluso nello SLA.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing k. Autenticazione a più fattori	Le agenzie devono implementare un'autenticazione a più fattori sufficien te quando le loro soluzioni cloud sono disponibili da Internet, ossia quando è possibile accedere alla soluzione cloud dall'esterno della rete affidabile dell'agenzia.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing k. Autenticazione a più fattori	Le agenzie devono implementare un'autenticazione a più fattori sufficien te quando le loro soluzioni cloud sono disponibili da Internet, ossia quando è possibile accedere alla soluzione cloud dall'esterno della rete affidabile dell'agenzia.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing k. Autenticazione a più fattori	Le agenzie devono implementare un'autenticazione a più fattori sufficien te quando le loro soluzioni cloud sono disponibili da Internet, ossia quando è possibile accedere alla soluzione cloud dall'esterno della rete affidabile dell'agenzia.	root-account-hardw are-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richieden do l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1 Cloud computing k. Autenticazione a più fattori	Le agenzie devono implementare un'autenticazione a più fattori sufficien te quando le loro soluzioni cloud sono disponibili da Internet, ossia quando è possibile accedere alla soluzione cloud dall'esterno della rete affidabile dell'agenzia.	root-account-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richieden do l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
3.3.1 Cloud computing i. Valutazio ne del rischio:	l'agenzia deve effettuare una valutazione annuale dei controlli di sicurezza e privacy in atto su tutti i sistemi informativi utilizzati per ricevere, elaborare, archiviare, accedere, protegger e e/o trasmettere gli FTI.	annual-risk-assess ment-performed(con trollo di processo)	Esegui una valutazio ne annuale del rischio sulla tua organizza zione. Le valutazioni del rischio possono aiutare a determina re la probabilità e l'impatto dei rischi e/o delle vulnerabi lità identificati che interessano un'organi zzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.6 Confine e infrastruttura di rete	Le agenzie devono implementare i dispositivi di protezion e dei confini in tutta la loro architettura di sistema, compresi router, firewall, switch e sistemi di rilevamen to delle intrusioni per proteggere l'FTI e i sistemi FTI.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.6 Confine e infrastruttura di rete	Le agenzie devono implementare i dispositivi di protezione e dei confini in tutta la loro architettura di sistema, compresi router, firewall, switch e sistemi di rilevamento delle intrusioni per proteggere l'FTI e i sistemi FTI.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.6 Confine e infrastruttura di rete	Le agenzie devono implementare i dispositivi di protezione e dei confini in tutta la loro architettura di sistema, compresi router, firewall, switch e sistemi di rilevamento delle intrusioni per proteggere l'FTI e i sistemi FTI.	netfw-policy-rule-group-associated	Una policy AWS Network Firewall definisce il modo in cui il firewall monitora e gestisce il traffico in un Amazon VPC. Puoi configurare gruppi di regole stateless e stateful per filtrare pacchetti e flussi di traffico, nonché definire la gestione del traffico predefinita.
3.3.6 Confine e infrastruttura di rete	Le agenzie devono implementare i dispositivi di protezione e dei confini in tutta la loro architettura di sistema, compresi router, firewall, switch e sistemi di rilevamento delle intrusioni per proteggere l'FTI e i sistemi FTI.	netfw-stateless-rule-group-not-empty	Un gruppo di regole AWS Network Firewall contiene regole che definiscono il modo in cui il firewall elabora il traffico nel tuo VPC. Un gruppo di regole stateless vuoto, se presente in una policy firewall, non elabora il traffico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.6 Confine e infrastruttura di rete	Le agenzie devono implementare i dispositivi di protezion e dei confini in tutta la loro architettura di sistema, compresi router, firewall, switch e sistemi di rilevamen to delle intrusioni per proteggere l'FTI e i sistemi FTI.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.6 Confine e infrastruttura di rete	Le agenzie devono implementare i dispositivi di protezione e dei confini in tutta la loro architettura di sistema, compresi router, firewall, switch e sistemi di rilevamento delle intrusioni per proteggere l'FTI e i sistemi FTI.	waf-regional-rule-not-empty	Assicurati che il tuo AWS WAF abbia una regola che non sia vuota. Una regola senza condizioni può comportare un comportamento non intenzionale.
3.3.6 Confine e infrastruttura di rete	Le agenzie devono implementare i dispositivi di protezione e dei confini in tutta la loro architettura di sistema, compresi router, firewall, switch e sistemi di rilevamento delle intrusioni per proteggere l'FTI e i sistemi FTI.	waf-regional-rulegroup-not-empty	Assicurati che il tuo AWS WAF abbia un gruppo di regole che non sia vuoto. Un gruppo di regole vuoto potrebbe causare un comportamento indesiderato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.6 Confine e infrastruttura di rete	Le agenzie devono implementare i dispositivi di protezion e dei confini in tutta la loro architettura di sistema, compresi router, firewall, switch e sistemi di rilevamen to delle intrusioni per proteggere l'FTI e i sistemi FTI.	waf-regional-webacl-not-empty	Un ACL Web allegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.
3.3.6 Confine e infrastruttura di rete	Le agenzie devono implementare i dispositivi di protezion e dei confini in tutta la loro architettura di sistema, compresi router, firewall, switch e sistemi di rilevamen to delle intrusioni per proteggere l'FTI e i sistemi FTI.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.6 Confine e infrastruttura di rete	Le agenzie devono implementare i dispositivi di protezione e dei confini in tutta la loro architettura di sistema, compresi router, firewall, switch e sistemi di rilevamento delle intrusioni per proteggere l'FTI e i sistemi FTI.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (f)	Creare, abilitare, modificare, disabilitare e rimuovere gli account in conformità ai prerequisiti delle procedure di gestione degli account delle agenzie;	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (f)	Creare, abilitare, modificare, disabilitare e rimuovere gli account in conformità ai prerequisiti delle procedure di gestione degli account delle agenzie;	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (f)	Creare, abilitare, modificare, disabilitare e rimuovere gli account in conformità ai prerequisiti delle procedure di gestione degli account delle agenzie;	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (f)	Creare, abilitare, modificare, disabilit are e rimuovere gli account in conformit à ai prerequisiti delle procedure di gestione degli account delle agenzie;	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (f)	Creare, abilitare, modificare, disabilitare e rimuovere gli account in conformità ai prerequisiti delle procedure di gestione degli account delle agenzie;	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (g)	Monitora l'uso degli account	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
Gestione account AC-2 (g)	Monitora l'uso degli account	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (g)	Monitora l'uso degli account	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail log. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (g)	Monitora l'uso degli account	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
Gestione account AC-2 (g)	Monitora l'uso degli account	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (g)	Monitora l'uso degli account	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (g)	Monitora l'uso degli account	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (g)	Monitora l'uso degli account	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (j)	Verifica la conformità degli account ai requisiti di gestione degli account	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (j)	Verifica la conformità degli account ai requisiti di gestione degli account	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (j)	Verifica la conformità degli account ai requisiti di gestione degli account	secretsmanager-secret-periodic-rotation	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione periodica abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto. Il valore predefinito è 90 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (j)	Verifica la conformità degli account ai requisiti di gestione degli account	secretsmanager-secret-unused	Se in AWS Secrets Manager sono presenti credenziali inutilizzate, è necessario disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola consente di impostare un valore su unusedForDays (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (j)	Verifica la conformità degli account ai requisiti di gestione degli account	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (j)	Verifica la conformità degli account ai requisiti di gestione degli account	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (j)	Verifica la conformità degli account ai requisiti di gestione degli account	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (j)	Verifica la conformità degli account ai requisiti di gestione degli account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (j)	Verifica la conformità degli account ai requisiti di gestione degli account	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (j)	Verifica la conformità degli account ai requisiti di gestione degli account	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
Gestione account AC-2 (j)	Verifica la conformità degli account ai requisiti di gestione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
(CE-1) Gestione automatizzata degli account di sistema	Supporta la gestione degli account di sistema utilizzando meccanismi automatizzati.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
(CE-1) Gestione automatizzata degli account di sistema	Supporta la gestione degli account di sistema utilizzando meccanismi automatizzati.	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
(CE-1) Gestione automatizzata degli account di sistema	Supporta la gestione degli account di sistema utilizzando meccanismi automatizzati.	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
(CE-3): disabilita account	Disabilita gli account entro 120 giorni se: a. Sono scaduti; b. Non sono più associati a un utente o a un individuo; c. Violano la policy dell'organizzazione; oppure d. Sono inattivi da 120 giorni per gli account privi di privilegi e da 60 giorni per gli account con privilegi	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
(CE-12) Monitoraggio degli account per usi atipici	Monitora gli account di sistema per verificare l'utilizz o atipico definito dall'agenzia e segnala l'utilizzo atipico degli account di sistema al personale o ai ruoli definiti dall'agenzia.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegio, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'organizzazione.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegio, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'organizzazione.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegio, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'organizzazione.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegio, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'organizzazione.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegio, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'organizzazione.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegio, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'organizzazione.	secretsmanager-secret-unused	Se in AWS Secrets Manager sono presenti credenziali inutilizzate, è necessario disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola consente di impostare un valore su unusedForDays (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegio, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'organizzazione.	codebuild-project-environment-privileged-check	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che il tuo ambiente di CodeBuild progetto Amazon non abbia la modalità privilegiata abilitata. Questa impostazione deve essere disabilitata per impedire l'accesso involontario alle API Docker e all'hardware sottostante del container.
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegio, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'organizzazione.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegio, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'organizzazione.	ecs-containers-nonprivileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegio, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'organizzazione.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegio, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'organizzazione.	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegio, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'organizzazione.	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegi o, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'orga nizzazione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
AC-6 Privilegio minimo	Utilizza il principio del minimo privilegi o, consentendo agli utenti (o ai processi che agiscono per conto degli utenti) solo gli accessi autorizzati necessari per svolgere le attività assegnate dall'orga nizzazione.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione e alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di gestione e le chiamate API. AWS È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17: accesso remoto	Stabilisci e documenta le limitazioni d'uso, i requisiti di configurazione/connessione e le linee guida per l'implementazione di ogni tipo di accesso remoto consentito; inoltre, autorizza ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
AT-1: sensibilizzazione e formazione	Offri una formazione sulla sicurezza e sulla privacy agli utenti del sistema (compresi i manager, i dirigenti e gli appaltatori).	security-awareness-program-exists (controllo di processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2: eventi di controllo	Identifica i tipi di eventi per cui il sistema è in grado di effettuare la registrazione di log a supporto della funzione di audit.	audit-log-policy-exists(controllo di processo)	Definizione e mantenimento di una policy di gestione dei log di audit che definisca i requisiti di gestione dei log dell'organizzazione. Ciò include, a titolo esemplificativo, la revisione e la conservazione dei log di audit.
AU-16: registrazione di log di audit inter-organizzativa	Utilizza metodi definiti dall'agenzia per coordinare le informazioni di audit definite dall'agenzia tra le organizzazioni esterne quando le informazioni di audit vengono trasmesse oltre i confini dell'organizzazione.	audit-log-policy-exists(controllo di processo)	Definizione e mantenimento di una policy di gestione dei log di audit che definisca i requisiti di gestione dei log dell'organizzazione. Ciò include, a titolo esemplificativo, la revisione e la conservazione dei log di audit.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7: monitoraggio continuo	Sviluppa una strategia di monitoraggio continuo a livello di sistema e implement a il monitoraggio continuo conformem ente a tale strategia a livello di organizza zione: definisci metriche da monitorar e stabilite dall'agen zia; valutazioni continue dei controlli conformi alla strategia di monitoraggio continuo; monitorag gio continuo delle metriche definite dal sistema e dall'organizzazion e in conformità alla strategia di monitorag gio continuo; correlazi one e analisi delle informazioni generate dalle valutazio ni dei controlli e dal monitoraggio; azioni di risposta per affrontare i risultati dell'anal isi delle informazi oni di valutazio	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ne e monitoraggio dei controlli; comunicazione dello stato di sicurezza e privacy del sistema al personale definito dall'agenzia, almeno una volta all'anno.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	aurora-resources-p rotected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	backup-plan-min-fr equency-and-min-re tention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservaz ione minime. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredF requencyValue (Config default: 1), (requiredRetentionD ays Config default: 35) e (requiredF requencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	backup-recovery-po int-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurat i che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionD ays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	dynamodb-pitr-enab led	Abilita questa regola per verificare che sia stato eseguito il backup delle informazi oni. Inoltre, mantiene i backup assicuran do che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristin o mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	ec2-resources-prot ected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	fsx-resources-prot ected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	rds-resources-prot ected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	redshift-backup-en abled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatiz zati. Quando gli snapshot automatic i sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazi one predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9: backup del sistema	a. Esegui il backup delle informazioni a livello di utente contenute nella documentazione del sistema, compresa quella relativa alla sicurezza, con cadenza settimanale; b. eseguire il backup delle informazioni a livello di sistema contenute nel sistema, con cadenza settimanale; c. eseguire backup della documentazione del sistema, compresa la documentazione relativa alla sicurezza e alla privacy, con cadenza settimana le; e d. proteggere la riservatezza, l'integri tà e la disponibilità delle informazioni di backup.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2: identificazione e autenticazione (utenti organizzativi) (CE-1) Autenticazione a più fattori su account con privilegi	Implementa l'autenticazione a più fattori per l'accesso agli account con privilegi	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2: identificazione e autenticazione (utenti organizzativi) (CE-1) Autenticazione a più fattori su account con privilegi	Implementa l'autenticazione a più fattori per l'accesso agli account con privilegi	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2: identificazione e autenticazione (utenti organizzativi) (CE-2) Autenticazione a più fattori su account senza privilegi	Implementa l'autenticazione a più fattori per l'accesso agli account senza privilegi.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-5: gestione degli autenticatori: (CE-1) autenticazione basata su password: per l'autenticazione basata su password	Applicare le seguenti regole di composizione e complessità: 1. Applicare una lunghezza minima della password di quattordici (14) caratteri. 2. Applicare una complessità minima della password che deve contenere una combinazione di numeri, lettere maiuscole, lettere minuscole e caratteri speciali. 3. Applicare la modifica di almeno un (1) carattere quando vengono selezionate nuove password da utilizzare. 4. Archiviare e trasmettere solo password protette crittograficamente. 5. Applicare le restrizioni sulla durata della password: i. Minimo un (1) giorno e massimo 90 giorni. ii. Le password degli account di servizio	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	scadono entro 366 giorni (inclusi).		Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PM-5: inventario di sistema	Sviluppa e aggiorna continuamente un inventario dei sistemi dell'organizzazione.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PM-5: inventario di sistema	Sviluppa e aggiorna continuamente un inventario dei sistemi dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PM-5: inventario di sistema	Sviluppa e aggiorna continuamente un inventario dei sistemi dell'organizzazione.	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PM-5: inventario di sistema	Sviluppa e aggiorna continuamente un inventario dei sistemi dell'organizzazione.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA-5: monitoraggio e scansione delle vulnerabilità	Monitorare e scansionare le vulnerabilità del sistema e delle applicazioni ospitate ogni trenta (30) giorni, prima di inserire un nuovo sistema informativo nella rete dell'agenzia, per confermare le azioni di rimedio e quando vengono identificate e segnalate nuove vulnerabilità che potrebbero interessa re il sistema	vuln-scans-perform ed(controllo di processo)	Assicurati che le scansioni delle vulnerabilità vengano eseguite in base ai requisiti di conformit à. La cadenza di scansione, gli strumenti utilizzat i e l'uso dei risultati devono essere definiti dall'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-10: gestione della configurazione per sviluppatori (e.)	Tieni traccia dei difetti di sicurezza e della risoluzione dei difetti all'interno del sistema, del componente o del servizio e segnala i risultati a [Assegnazione: personale definito dall'organizzazione].	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-10: gestione della configurazione per sviluppatori (e.)	Tieni traccia dei difetti di sicurezza e della risoluzione dei difetti all'interno del sistema, del componente o del servizio e segnala i risultati a [Assegnazione: personale definito dall'organizzazione].	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-10: gestione della configurazione per sviluppatori (e.)	Tieni traccia dei difetti di sicurezza e della risoluzione dei difetti all'interno del sistema, del componente o del servizio e segnala i risultati a [Assegnazione: personale definito dall'organizzazione].	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-10: gestione della configurazione per sviluppatori (a) (c.)	Esegui la gestione della configurazione durante la progettazione, lo sviluppo, l'implementazione e il funzionamento di sistemi, componenti o servizi; implementa solo le modifiche approvate dall'organizzazione al sistema, al componente o al servizio;	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-4: informazioni nelle risorse di sistema condivise	Previeni il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini	Monitora e controlla le comunicazioni ai confini esterni del sistema e ai confini chiave interni all'interno del sistema; implementa sottoreti per i componenti del sistema accessibili al pubblico e separate dalle reti organizzative interne; connettiti a reti o sistemi informativi esterni solo attraverso interfacce gestite costituite da dispositivi di protezione dei confini disposti in conformità a un'architettura di sicurezza organizzativa.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini	Monitora e controlla le comunicazioni ai confini esterni del sistema e ai confini chiave interni all'interno del sistema; implementa sottoreti per i componenti del sistema accessibili al pubblico e separate dalle reti organizzative interne; connettiti a reti o sistemi informativi esterni solo attraverso interfacce gestite costituite da dispositivi di protezione dei confini disposti in conformità a un'architettura di sicurezza organizzativa.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini	Monitora e controlla le comunicazioni ai confini esterni del sistema e ai confini chiave interni all'interno del sistema; implementa sottoreti per i componenti del sistema accessibili al pubblico e separate dalle reti organizzative interne; connettiti a reti o sistemi informativi esterni solo attraverso interfacce gestite costituite da dispositivi di protezione dei confini disposti in conformità a un'architettura di sicurezza organizzativa.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini	Monitora e controlla le comunicazioni ai confini esterni del sistema e ai confini chiave interni all'interno del sistema; implementa sottoreti per i componenti del sistema accessibili al pubblico e separate dalle reti organizzative interne; connettiti a reti o sistemi informativi esterni solo attraverso interfacce gestite costituite da dispositivi di protezione dei confini disposti in conformità a un'architettura di sicurezza organizzativa.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini	Monitora e controlla le comunicazioni ai confini esterni del sistema e ai confini chiave interni all'interno del sistema; implementa sottoreti per i componenti del sistema accessibili al pubblico e separate dalle reti organizzative interne; connettiti a reti o sistemi informativi esterni solo attraverso interfacce gestite costituite da dispositivi di protezione dei confini disposti in conformità a un'architettura di sicurezza organizzativa.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini	Monitora e controlla le comunicazioni ai confini esterni del sistema e ai confini chiave interni all'interno del sistema; implementa sottoreti per i componenti del sistema accessibili al pubblico e separate dalle reti organizzative interne; connettiti a reti o sistemi informativi esterni solo attraverso interfacce gestite costituite da dispositivi di protezione dei confini disposti in conformità a un'architettura di sicurezza organizzativa.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini	Monitora e controlla le comunicazioni ai confini esterni del sistema e ai confini chiave interni all'interno del sistema; implementa sottoreti per i componenti del sistema accessibili al pubblico e separate dalle reti organizzative interne; connettiti a reti o sistemi informativi esterni solo attraverso interfacce gestite costituite da dispositivi di protezione dei confini disposti in conformità a un'architettura di sicurezza organizzativa.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini	Monitora e controlla le comunicazioni ai confini esterni del sistema e ai confini chiave interni all'interno del sistema; implementa sottoreti per i componenti del sistema accessibili al pubblico e separate dalle reti organizzative interne; connettiti a reti o sistemi informativi esterni solo attraverso interfacce gestite costituite da dispositivi di protezione dei confini disposti in conformità a un'architettura di sicurezza organizzativa.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini	Monitora e controlla le comunicazioni ai confini esterni del sistema e ai confini chiave interni all'interno del sistema; implementa sottoreti per i componenti del sistema accessibili al pubblico e separate dalle reti organizzative interne; connettiti a reti o sistemi informativi esterni solo attraverso interfacce gestite costituite da dispositivi di protezione dei confini disposti in conformità a un'architettura di sicurezza organizzativa.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini	Monitora e controlla le comunicazioni ai confini esterni del sistema e ai confini chiave interni all'interno del sistema; implementa sottoreti per i componenti del sistema accessibili al pubblico e separate dalle reti organizzative interne; connettiti a reti o sistemi informativi esterni solo attraverso interfacce gestite costituite da dispositivi di protezione dei confini disposti in conformità a un'architettura di sicurezza organizzativa.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini	Monitora e controlla le comunicazioni ai confini esterni del sistema e ai confini chiave interni all'interno del sistema; implementa sottoreti per i componenti del sistema accessibili al pubblico e separate dalle reti organizzative interne; connettiti a reti o sistemi informativi esterni solo attraverso interfacce gestite costituite da dispositivi di protezione dei confini disposti in conformità a un'architettura di sicurezza organizzativa.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini	Monitora e controlla le comunicazioni ai confini esterni del sistema e ai confini chiave interni all'interno del sistema; implementa sottoreti per i componenti del sistema accessibili al pubblico e separate dalle reti organizzative interne; connettiti a reti o sistemi informativi esterni solo attraverso interfacce gestite costituite da dispositivi di protezione dei confini disposti in conformità a un'architettura di sicurezza organizzativa.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini (CE-9) Limitazione del traffico di comunicazioni minacciose in uscita	Rileva e respingi il traffico di comunicazioni in uscita che rappresenta una minaccia per i sistemi esterni e verifica l'identità degli utenti interni associati alle comunicazioni negate.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini (CE-9) Limitazione del traffico di comunicazioni minacciose in uscita	Rileva e respingi il traffico di comunicazioni in uscita che rappresenta una minaccia per i sistemi esterni e verifica l'identità degli utenti interni associati alle comunicazioni negate.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini (CE-9) Limitazione del traffico di comunicazioni minacciose in uscita	Rileva e respingi il traffico di comunicazioni in uscita che rappresenta una minaccia per i sistemi esterni e verifica l'identità degli utenti interni associati alle comunicazioni negate.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
SC-7: protezione dei confini (definita da IRS)	Le agenzie devono implementare e gestire la protezione dei confini (in genere utilizzando firewall) ai limiti di attendibilità. È necessario monitorare ogni limite di attendibilità e controllare le comunicazioni attraverso ciascun limite.	netfw-policy-rule-group-associated	Una policy AWS Network Firewall definisce il modo in cui il firewall monitora e gestisce il traffico in un Amazon VPC. Puoi configurare gruppi di regole stateless e stateful per filtrare pacchetti e flussi di traffico, nonché definire la gestione del traffico predefinita.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7: protezione dei confini (definita da IRS)	Le agenzie devono implementare e gestire la protezione dei confini (in genere utilizzando firewall) ai limiti di attendibilità. È necessario monitorare ogni limite di attendibilità e controllare le comunicazioni attraverso ciascun limite.	netfw-stateless-rule-group-not-empty	Un gruppo di regole AWS Network Firewall contiene regole che definiscono il modo in cui il firewall elabora il traffico nel tuo VPC. Un gruppo di regole stateless vuoto, se presente in una policy firewall, non elabora il traffico.
SC-8: riservatezza e integrità della trasmissione (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione non autorizzata di informazioni e rilevare le modifiche alle informazioni durante la trasmissione.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8: riservatezza e integrità della trasmissione (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione non autorizzata di informazioni e rilevare le modifiche alle informazioni durante la trasmissione.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8: riservatezza e integrità della trasmissione (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione non autorizzata di informazioni e rilevare le modifiche alle informazioni durante la trasmissione.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8: riservatezza e integrità della trasmissione (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione non autorizzata di informazioni e rilevare le modifiche alle informazioni durante la trasmissione.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
SC-8: riservatezza e integrità della trasmissione (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione non autorizzata di informazioni e rilevare le modifiche alle informazioni durante la trasmissione.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8: riservatezza e integrità della trasmissione (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione non autorizzata di informazioni e rilevare le modifiche alle informazioni durante la trasmissione.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8: riservatezza e integrità della trasmissione (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione non autorizzata di informazioni e rilevare le modifiche alle informazioni durante la trasmissione.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12: creazione e gestione delle chiavi crittografiche	L'agenzia deve stabilire e gestire le chiavi crittografiche quando la crittografia è utilizzata all'interno del sistema conformemente ai seguenti requisiti di gestione delle chiavi: NIST SP 800-57, Suggerimento per la gestione delle chiavi, per la generazione, la distribuzione, l'archiviazione, l'accesso e la distruzione delle chiavi.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che le chiavi master del cliente (CMK) necessarie non siano pianificate per l'eliminazione in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12: creazione e gestione delle chiavi crittografiche	L'agenzia deve stabilire e gestire le chiavi crittografiche quando la crittografia è utilizzata all'interno del sistema conformemente ai seguenti requisiti di gestione delle chiavi: NIST SP 800-57, Suggerimento per la gestione delle chiavi, per la generazione, la distribuzione, l'archiviazione, l'accesso e la distruzione delle chiavi.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	opensearch-encrypt ed-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalidato FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implementazioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalidato FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implementazioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	elasticsearch-encr ypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalidato FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implementazioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13: protezione crittografica	Implementa i seguenti tipi di crittografia richiesti per ogni uso crittografico: ultimo meccanismo di crittografia convalida to FIPS-140, NIST 800-52, Linee guida per la selezione, la configurazione e l'uso delle implement azioni Transport Layer Security (TLS), Crittografia in transito (crittografia del payload). L'uso di SHA-1 per le firme digitali è vietato.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23: autenticità della sessione	Protezione dell'autenticità delle sessioni di comunicazione.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28: protezione delle informazioni a riposo (CE-1) Protezione crittografica	Implementa meccanismi crittografici per impedire la divulgazione e la modifica non autorizzate di FTI a riposo sui sistemi informatici degli utenti finali (ad esempio computer desktop, computer portatili, dispositivi mobili, dispositivi di archiviazione portatili e rimovibili) in archiviazione non volatile.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2: correzione dei difetti (definita da IRS)	L'agenzia deve garantire che, al momento dell'accensione e della connessione giornaliere alla rete dell'agenzia, le postazioni di lavoro (come definite nella politica e comprese le connessioni remote tramite workstation GFE) siano controllate per garantire che siano state applicate le patch più recenti approvate dall'agenzia e che tutte le patch assenti o nuove vengano applicate secondo necessità o altrimenti controllate non meno di ogni 24 ore (esclusi i fine settimana, i giorni festivi, ecc.)	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2: correzione dei difetti (definita da IRS)	L'agenzia deve garantire che, al momento dell'accensione e della connessione giornaliere alla rete dell'agenzia, le postazioni di lavoro (come definite nella politica e comprese le connessioni remote tramite workstation GFE) siano controllate per garantire che siano state applicate le patch più recenti approvate dall'agenzia e che tutte le patch assenti o nuove vengano applicate secondo necessità o altrimenti controllate non meno di ogni 24 ore (esclusi i fine settimana, i giorni festivi, ecc.)	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2: correzione dei difetti (definita da IRS)	L'agenzia deve garantire che, al momento dell'accensione e della connessione giornaliere alla rete dell'agenzia, le postazioni di lavoro (come definite nella politica e comprese le connessioni remote tramite workstation GFE) siano controllate per garantire che siano state applicate le patch più recenti approvate dall'agenzia e che tutte le patch assenti o nuove vengano applicate secondo necessità o altrimenti controllate non meno di ogni 24 ore (esclusi i fine settimana, i giorni festivi, ecc.)	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2: correzione dei difetti (definita da IRS)	L'agenzia deve garantire che, al momento dell'acce nsione e della connessione giornalie re alla rete dell'agen zia, le postazion i di lavoro (come definite nella politica e comprese le connessioni remote tramite workstation GFE) siano controlla te per garantire che siano state applicate le patch più recenti approvate dall'agen zia e che tutte le patch assenti o nuove vengano applicate secondo necessità o altrimenti controlla te non meno di ogni 24 ore (esclusi i fine settimana, i giorni festivi, ecc.)	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribuiti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2: correzione dei difetti (definita da IRS)	L'agenzia deve garantire che, al momento dell'accensione e della connessione giornaliere alla rete dell'agenzia, le postazioni di lavoro (come definite nella politica e comprese le connessioni remote tramite workstation GFE) siano controllate per garantire che siano state applicate le patch più recenti approvate dall'agenzia e che tutte le patch assenti o nuove vengano applicate secondo necessità o altrimenti controllate non meno di ogni 24 ore (esclusi i fine settimana, i giorni festivi, ecc.)	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2: correzione dei difetti (definita da IRS)	L'agenzia deve garantire che, al momento dell'accensione e della connessione giornaliere alla rete dell'agenzia, le postazioni di lavoro (come definite nella politica e comprese le connessioni remote tramite workstation GFE) siano controllate per garantire che siano state applicate le patch più recenti approvate dall'agenzia e che tutte le patch assenti o nuove vengano applicate secondo necessità o altrimenti controllate non meno di ogni 24 ore (esclusi i fine settimana, i giorni festivi, ecc.)	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi conformem ente a [Assegnaz ione: obiettivi di monitoraggio definiti dall'organizzazion e]; e 2. Connessio ni locali, di rete e remote non autorizza te; b. Identifica l'uso non autorizza to del sistema informativo attravers o [Assegnazione: tecniche e metodi definiti dall'orga nizzazione]; c. Implementa dispositi vi di monitorag gio: 1. Strategic amente all'interno del sistema informati vo per raccoglie re le informazioni essenziali determina te dall'organizzazion e. In posizioni ad hoc all'interno del sistema per tracciare tipi	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	specifici di transazioni di interesse per l'organizzazione; d. protegge le informazioni ottenute dagli strumenti di monitoraggio delle intrusioni da accessi, modifiche e cancellazioni non autorizzati;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenziali attacchi conformemente a [Assegnazione: obiettivi di monitoraggio definiti dall'organizzazione]; e 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnazione: tecniche e metodi definiti dall'organizzazione]; c. Implementa dispositivi di monitoraggio: 1. Strategicamente all'interno del sistema informativo per raccogliere le informazioni essenziali determinate dall'organizzazione. In posizioni ad hoc all'interno del sistema per tracciare tipi	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	specifici di transazioni di interesse per l'organizzazione; d. protegge le informazioni ottenute dagli strumenti di monitoraggio delle intrusioni da accessi, modifiche e cancellazioni non autorizzati;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenziali attacchi conformemente a [Assegnazione: obiettivi di monitoraggio definiti dall'organizzazione]; e 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnazione: tecniche e metodi definiti dall'organizzazione]; c. Implementa dispositivi di monitoraggio: 1. Strategicamente all'interno del sistema informativo per raccogliere le informazioni essenziali determinate dall'organizzazione. In posizioni ad hoc all'interno del sistema per tracciare tipi	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	specifici di transazioni di interesse per l'organizzazione; d. protegge le informazioni ottenute dagli strumenti di monitoraggio delle intrusioni da accessi, modifiche e cancellazioni non autorizzati;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi conformem ente a [Assegnaz ione: obiettivi di monitoraggio definiti dall'organizzazion e]; e 2. Connessio ni locali, di rete e remote non autorizza te; b. Identifica l'uso non autorizza to del sistema informativo attravers o [Assegnazione: tecniche e metodi definiti dall'orga nizzazione]; c. Implementa dispositi vi di monitorag gio: 1. Strategic amente all'interno del sistema informati vo per raccoglie re le informazioni essenziali determina te dall'organizzazion e. In posizioni ad hoc all'interno del sistema per tracciare tipi	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	specifici di transazioni di interesse per l'organizzazione; d. protegge le informazioni ottenute dagli strumenti di monitoraggio delle intrusioni da accessi, modifiche e cancellazioni non autorizzati;		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenziali attacchi conformemente a [Assegnazione: obiettivi di monitoraggio definiti dall'organizzazione]; e 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnazione: tecniche e metodi definiti dall'organizzazione]; c. Implementa dispositivi di monitoraggio: 1. Strategicamente all'interno del sistema informativo per raccogliere le informazioni essenziali determinate dall'organizzazione. In posizioni ad hoc all'interno del sistema per tracciare tipi	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	specifici di transazioni di interesse per l'organizzazione; d. protegge le informazioni ottenute dagli strumenti di monitoraggio delle intrusioni da accessi, modifiche e cancellazioni non autorizzati;		
SI-4: monitoraggio del sistema (definito da IRS)	Tutti i punti/portali di accesso a Internet devono acquisire e conservare, per almeno un anno, le informazioni sulle intestazioni del traffico in entrata e in uscita, con l'esclusione delle connessioni "anonime" a Internet approvate, che possono essere approvate dal CISO dell'agenzia.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema (definito da IRS)	Tutti i punti/portali di accesso a Internet devono acquisire e conservare, per almeno un anno, le informazioni sulle intestazioni del traffico in entrata e in uscita, con l'esclusione delle connessioni "anonime" a Internet approvate, che possono essere approvate dal CISO dell'agenzia.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema (definito da IRS)	Tutti i punti/portali di accesso a Internet devono acquisire e conservare, per almeno un anno, le informazioni sulle intestazioni del traffico in entrata e in uscita, con l'esclusione delle connessioni "anonime" a Internet approvate, che possono essere approvate dal CISO dell'agenzia.	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema (definito da IRS)	Tutti i punti/portali di accesso a Internet devono acquisire e conservare, per almeno un anno, le informazioni sulle intestazioni del traffico in entrata e in uscita, con l'esclusione delle connessioni "anonime" a Internet approvate, che possono essere approvate dal CISO dell'agenzia.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema (definito da IRS)	Tutti i punti/portali di accesso a Internet devono acquisire e conservare, per almeno un anno, le informazioni sulle intestazioni del traffico in entrata e in uscita, con l'esclusione delle connessioni "anonime" a Internet approvate, che possono essere approvate dal CISO dell'agenzia.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema (definito da IRS)	Tutti i punti/portali di accesso a Internet devono acquisire e conservare, per almeno un anno, le informazioni sulle intestazioni del traffico in entrata e in uscita, con l'esclusione delle connessioni "anonime" a Internet approvate, che possono essere approvate dal CISO dell'agenzia.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
SI-4: monitoraggio del sistema (definito da IRS)	Tutti i punti/portali di accesso a Internet devono acquisire e conservare, per almeno un anno, le informazioni sulle intestazioni del traffico in entrata e in uscita, con l'esclusione delle connessioni "anonime" a Internet approvate, che possono essere approvate dal CISO dell'agenzia.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema (definito da IRS)	Tutti i punti/portali di accesso a Internet devono acquisire e conservare, per almeno un anno, le informazioni sulle intestazioni del traffico in entrata e in uscita, con l'esclusione delle connessioni "anonime" a Internet approvate, che possono essere approvate dal CISO dell'agenzia.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema (definito da IRS)	Tutti i punti/portali di accesso a Internet devono acquisire e conservare, per almeno un anno, le informazioni sulle intestazioni del traffico in entrata e in uscita, con l'esclusione delle connessioni "anonime" a Internet approvate, che possono essere approvate dal CISO dell'agenzia.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema (definito da IRS)	Tutti i punti/portali di accesso a Internet devono acquisire e conservare, per almeno un anno, le informazioni sulle intestazioni del traffico in entrata e in uscita, con l'esclusione delle connessioni "anonime" a Internet approvate, che possono essere approvate dal CISO dell'agenzia.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail log. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4: monitoraggio del sistema (definito da IRS)	Tutti i punti/portali di accesso a Internet devono acquisire e conservare, per almeno un anno, le informazioni sulle intestazioni del traffico in entrata e in uscita, con l'esclusione delle connessioni "anonime" a Internet approvate, che possono essere approvate dal CISO dell'agenzia.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7: integrità del software, del firmware e delle informazioni	Utilizza strumenti di verifica dell'integrità per rilevare modifiche non autorizzate ai seguenti software, firmware e informazioni: kernel di sistema, driver, firmware (ad esempio BIOS, UEFI), software (ad esempio, sistema operativo, applicazioni, middleware) e attributi di sicurezza.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7: integrità del software, del firmware e delle informazioni	Utilizza strumenti di verifica dell'integrità per rilevare modifiche non autorizzate ai seguenti software, firmware e informazioni: kernel di sistema, driver, firmware (ad esempio BIOS, UEFI), software (ad esempio, sistema operativo, applicazioni, middleware) e attributi di sicurezza.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7: integrità del software, del firmware e delle informazioni	Utilizza strumenti di verifica dell'integrità per rilevare modifiche non autorizzate ai seguenti software, firmware e informazioni: kernel di sistema, driver, firmware (ad esempio BIOS, UEFI), software (ad esempio, sistema operativo, applicazioni, middleware) e attributi di sicurezza.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	dynamodb-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	ebs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	efs-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	rds-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le risorse di Amazon Relational Database Service (Amazon RDS) facciano parte di un AWS piano di backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'inter no del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi , direttive, regolamen ti, policy, standard, linee guida e requisiti operativi applicabili.	backup-recovery-po int-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	s3-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12: Gestione e conservazione delle informazioni	Gestisci e conserva le informazioni all'interno del sistema e le informazioni in uscita dal sistema conformemente a leggi, ordini esecutivi, direttive, regolamenti, policy, standard, linee guida e requisiti operativi applicabili.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for IRS 1075.

Best practice operative per K-ISMS

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra Corea: Information Security Management System (ISMS) e regole Config AWS gestite. Ogni regola di configurazione si applica a una risorsa AWS specifica e si riferisce a uno o più controlli Korea – ISMS. Un controllo Korea può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	AWS Regola di Config	Linea guida
1.2.1	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.
1.2.1	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.
2.1.3	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di

ID controllo	AWS Regola di Config	Linea guida
		un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configura zioni delle applicazioni e altri dettagli sull'ambiente.
2.1.3	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'elimina zione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata , potrebbe violare il concetto di funzionalità minima.
2.3.3	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatc h per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusi one dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
2.3.3	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di Config	Linea guida
2.5.1	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
2.5.1	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
2.5.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
2.5.1	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizza zioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
2.5.1	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
2.5.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
2.5.1	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
2.5.1	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
2.5.1	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
2.5.1	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibili tà che un'identità riceva o mantenga privilegi eccessivi.
2.5.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	AWS Regola di Config	Linea guida
2.5.1	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
2.5.1	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
2.5.1	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.
2.5.3	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
2.5.3	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
2.5.3	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
2.5.4	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
2.5.5	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associa zione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.
2,5,5	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
2.5.5	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
2.6	alb-waf-enabled	Assicurati che il AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di Config	Linea guida
2.6	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.
2.6	ebs-snapshot-public-restora ble-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
2.6	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
2.6	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
2.6	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
2.6	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
2.6	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
2.6	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
2.6	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
2.6	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
2.6	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
2.6	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.
2.6	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
2.6	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
2.6	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Regola di Config	Linea guida
2.6	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
2.6	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
2.6	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtraggio basato sullo stato del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di Config	Linea guida
2.6	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
2.6.6	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	AWS Regola di Config	Linea guida
2.6.6	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
2.6.6	lambda-function-public-acce ss-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.
2.6.6	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
2.6.6	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
2.6.6	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
2.6.6	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
2.6.6	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Regola di Config	Linea guida
2.6.6	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
2.6.6	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
2.6.6	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtraggio basato sullo stato del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di Config	Linea guida
2.6.6	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
2.6.7	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
2.7	acm-certificate-expiration-check	Garantisci la protezione e dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
2.7	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
2.7	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
2.7	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
2.7	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
2.7	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
2.7	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	AWS Regola di Config	Linea guida
2.7	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
2.7	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
2.7	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	AWS Regola di Config	Linea guida
2.7	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
2.7	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
2.7	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
2.7	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
2.7	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
2.7	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
2.7	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.
2.7	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
2.7	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
2.7	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
2.7	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
2.7	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
2.7	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
2.7	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	AWS Regola di Config	Linea guida
2.7	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
2.7.1	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire e ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	AWS Regola di Config	Linea guida
2.7.1	elb-predefined-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che gli ascoltatori SSL Classic Elastic Load Balancing utilizzino una policy di sicurezza predefinita. Elastic Load Balancing fornisce configurazioni di negoziazione SSL predefinite, che vengono utilizzate per la negoziazione SSL quando viene stabilita una connessione tra un client e il load balancer. Le configurazioni di negoziazione SSL garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi di crittografia altamente sicuri. Questa regola richiede l'impostazione di una policy di sicurezza predefinita per gli ascoltatori SSL. La politica di sicurezza predefinita è: SecurityPolicy ELB -TLS-1-2-2017-0. Il valore effettivo deve essere conforme alle policy dell'organizzazione.
2.7.2	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	AWS Regola di Config	Linea guida
2.7.2	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
2.8.5	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	AWS Regola di Config	Linea guida
2.8.5	codebuild-project-source-repo-url-check	Assicurati che l' GitHub URL del repository di origine di Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub
2.8.6	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	AWS Regola di Config	Linea guida
2.8.6	codebuild-project-source-repo-url-check	Assicurati che l' GitHub URL del repository di origine di Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub
2.9.1	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportar e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
2.9.1	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrai l, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittogra fia dei log, la convalida dei log e l'abilitazione AWS CloudTrai l in più aree.

ID controllo	AWS Regola di Config	Linea guida
2.9.1	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrai l Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	AWS Regola di Config	Linea guida
2.9.1	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
2.9.2	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	AWS Regola di Config	Linea guida
29.2	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
2.9.2	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCU Threshold Percentage (Config Default: 80) e AccountWCU Threshold Percentage (Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
2.9.2	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.
29.2	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	AWS Regola di Config	Linea guida
29.2	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.
29.3	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	AWS Regola di Config	Linea guida
29.3	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
2.9.3	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
2.9.3	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
2.9.3	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
2.9.3	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.
2.9.3	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di Config	Linea guida
29.3	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
29.3	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di Config	Linea guida
29.3	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
2.9.3	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di Config	Linea guida
29.3	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
29.3	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	AWS Regola di Config	Linea guida
29.3	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.

ID controllo	AWS Regola di Config	Linea guida
29.3	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	AWS Regola di Config	Linea guida
29.3	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
2.9.3	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
2.9.4	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
2,9,4	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
2.9.4	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
2.9.4	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
2.9.4	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	AWS Regola di Config	Linea guida
2,9,4	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di Config	Linea guida
2,9,4	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
2.9.4	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
2,9,4	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuat e a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richieden te, nome del bucket, ora della richiesta, azione della richiesta , stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di Config	Linea guida
2,9,4	vpc-flow-logs-enabled	I log di flusso VPC forniscon o record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
2,9,4	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di Config	Linea guida
2.10.3	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'elimina zione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata , potrebbe violare il concetto di funzionalità minima.
210.3	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
2.10.3	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.
2.10.3	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
2.10.3	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.
2,10,5	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
2,10,5	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittogra fate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
2,10,5	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
2.10.5	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
2.10.5	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
2,10,5	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
2,10,5	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
2,10,5	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
2.10.8	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.
2.10.8	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
2.11.2	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
2.11.3	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.
2.11.3	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	AWS Regola di Config	Linea guida
2.11.3	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
2.11.3	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultane ità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	AWS Regola di Config	Linea guida
2.11.3	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	AWS Regola di Config	Linea guida
2.11.3	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
2.12	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservaz ione specifici per soddisfare i requisiti di resilienza.

ID controllo	AWS Regola di Config	Linea guida
2,12	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
2.12	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
2.12	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
2.12	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
2.12	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.
2.12	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di Config	Linea guida
2,12	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
2,12	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di Config	Linea guida
2,12	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
2.12	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di Config	Linea guida
2,12	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.
2.12	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
2,12	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
2,12	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.

ID controllo	AWS Regola di Config	Linea guida
2,12	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	AWS Regola di Config	Linea guida
2,12	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
2.12	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfar e i requisiti di conformit à aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyV alue (Config default: 1), (requiredRetentionD ays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for K-ISMS.

Best practice operative per il bilanciamento del carico

Questo pacchetto di conformità contiene AWS Config regole basate sul bilanciamento del carico all'interno. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle AWS Config regole gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Load Balancing.

Best practice operative per la registrazione

Questo pacchetto di conformità contiene AWS Config regole basate sull'accesso. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle AWS Config regole gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Logging.

Best practice operative per i servizi di gestione e governance

Questo pacchetto di conformità contiene AWS Config regole basate sui servizi di gestione e governance. Per ulteriori informazioni, vedere Management and Governance su. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Management and Governance Services.

Best practice operative per MAS Notice 655

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra la Notice 655 dell'Autorità Monetaria di Singapore (MAS) — Cyber Hygiene e le regole di AWS Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli MAS Notice 655 — Cyber Hygiene. Un MAS Notice 655 – Il controllo Cyber Hygiene può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	AWS Regola di Config	Linea guida
4.1	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibili tà che un'identità riceva o mantenga privilegi eccessivi.
4.1	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza . Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
4.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può

ID controllo	AWS Regola di Config	Linea guida
		aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	AWS Regola di Config	Linea guida
4.1	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
4.1	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
4.1	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associa zione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
4.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
4.1	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
4.1	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
4.1	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
4.1	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
4.1	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
4.1	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
4.1	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
4.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
4.1	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.
4.1	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizza zioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
4.1	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.
4.1	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
4.1	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
4.2	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
4.2	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
4.2	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
4.2	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
4.2	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per protegger e l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
4.2	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornamenti, correzion i e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	AWS Regola di Config	Linea guida
4.2	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.
4.2	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilitazione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

ID controllo	AWS Regola di Config	Linea guida
4.3	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
4.3	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
4.3	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.
4.3	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	AWS Regola di Config	Linea guida
4.4	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
4.4	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicam ente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
4.4	ebs-snapshot-public-restora ble-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
4.4	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
4.4	ec2-security-group-attached-to-eni-periodic	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanz a Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambiente.

ID controllo	AWS Regola di Config	Linea guida
4.4	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
4.4	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
4.4	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
4.4	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
4.4	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
4.4	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
4.4	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
4.4	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
4.4	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
4.4	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
4.4	waf-regional-rule-not-empty	Assicurati che il tuo AWS WAF abbia una regola che non sia vuota. Una regola senza condizioni può comportare un comportamento non intenzionale.

ID controllo	AWS Regola di Config	Linea guida
4.4	waf-regional-rulegroup-not-empty	Assicurati che il tuo AWS WAF abbia un gruppo di regole che non sia vuoto. Un gruppo di regole vuoto potrebbe causare un comportamento indesider ato.
4.4	waf-regional-webacl-not-empty	Un ACL Web collegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.
4.4	netfw-policy-default-action-fragment-packets	Una policy AWS Network Firewall definisce il modo in cui il firewall monitora e gestisce il traffico in un Amazon VPC. Puoi configura re gruppi di regole stateless e stateful per filtrare pacchetti e flussi di traffico. L'imposta zione predefinita di un'azione Pass può consentire traffico indesiderato.

ID controllo	AWS Regola di Config	Linea guida
4.4	netfw-policy-default-action-full-packets	Una policy AWS Network Firewall definisce il modo in cui il firewall monitora e gestisce il traffico in un Amazon VPC. Puoi configura re gruppi di regole stateless e stateful per filtrare pacchetti e flussi di traffico. L'imposta zione predefinita di un'azione Pass può consentire traffico indesiderato.
4.4	netfw-policy-rule-group-ass ociated	Una policy AWS Network Firewall definisce il modo in cui il firewall monitora e gestisce il traffico in un Amazon VPC. Puoi configura re gruppi di regole stateless e stateful per filtrare pacchetti e flussi di traffico, nonché definire la gestione del traffico predefinita.
4.4	netfw-stateless-rule-group-not-empty	Un gruppo di regole AWS Network Firewall contiene regole che definiscono il modo in cui il firewall elabora il traffico nel tuo VPC. Un gruppo di regole stateless vuoto, se presente in una policy firewall, non elabora il traffico.

ID controllo	AWS Regola di Config	Linea guida
4.4	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
4.4	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
4.4	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
4.4	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
4.4	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS
4.4	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di Config	Linea guida
4.4	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
4.4	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
4.4	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
4.4	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
4.4	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	AWS Regola di Config	Linea guida
4.4	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
4.4	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	AWS Regola di Config	Linea guida
4.4	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
4.4	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	AWS Regola di Config	Linea guida
4.4	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
4.5	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
4.5	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
4.5	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
4.5	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
4.6	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
4.6	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
4.6	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
4.6	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
4.6	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
4.6	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for MAS Notice 655.

Best practice operative per MAS TRMG

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra le Linee guida per la gestione dei rischi tecnologici (TRMG) dell'Autorità monetaria di Singapore (MAS) del gennaio 2021 e le regole di AWS Config gestite. Ogni regola AWS Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli MAS TRMG. Un controllo MAS TRMG di gennaio 2021 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	AWS Regola di Config	Linea guida
3.3.1	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportar e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
5.4.3	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviar e queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.
5.4.3	codebuild-project-source-repo-url-check	Assicurati che l' GitHub URL del repository di origine di Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione

ID controllo	AWS Regola di Config	Linea guida
		all'accesso ai repository Bitbucket. GitHub
6.1.1	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.
6.1.2	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	AWS Regola di Config	Linea guida
6.1.4	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
6.1.4	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
6.1.4	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
6.2.1	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	AWS Regola di Config	Linea guida
6.3.1	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.
6,4,5	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
6.4.5	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
6,4,5	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
6,4,5	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	AWS Regola di Config	Linea guida
6.4.5	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
6.4.5	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
6.4.5	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	AWS Regola di Config	Linea guida
6.4.5	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
6.4.5	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
6,4,5	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Regola di Config	Linea guida
6.4.5	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
6,4,5	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
6.4.6	api-gw-execution-logging-en abled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	AWS Regola di Config	Linea guida
6.4.6	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
6.4.6	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di Config	Linea guida
6.4.6	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrai l Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	AWS Regola di Config	Linea guida
6.4.6	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di Config	Linea guida
6.4.6	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
6.4.6	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
6.4.6	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
6.4.6	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di Config	Linea guida
6.4.6	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
6.4.7	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
6.4.7	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
6.4.7	cloudtrail-enabled	AWS CloudTrail può contribui re a evitare il ripudio registran do le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizz ati in AWS CloudTrail Record Contents.
6.4.7	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrai l Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	AWS Regola di Config	Linea guida
6.4.7	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
6.4.7	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
6.4.7	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	AWS Regola di Config	Linea guida
6.4.7	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
6.4.7	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
6.4.7	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
6.4.7	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
6.4.7	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
6.4.7	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di Config	Linea guida
6.4.7	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
6.4.7	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di Config	Linea guida
6.4.8	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
6.4.8	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	AWS Regola di Config	Linea guida
6.4.8	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.
6.4.8	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di Config	Linea guida
6.4.8	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
6.4.8	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di Config	Linea guida
6.4.8	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di Config	Linea guida
6.4.8	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	AWS Regola di Config	Linea guida
7.2.1	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
7.2.1	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
7.4.1	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
7.4.1	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	AWS Regola di Config	Linea guida
7.4.1	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
7.4.1	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	AWS Regola di Config	Linea guida
7.4.1	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	AWS Regola di Config	Linea guida
7.4.1	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
7.5.5	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
7,5,5	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
7.5.5	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
7.5.5	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
7.5.5	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
7.5.5	elasticache-redis-cluster-a utomatic-backup-check	Quando i backup automatic i sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornalie ra. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazion e. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	AWS Regola di Config	Linea guida
7.5.5	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
7.5.5	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	AWS Regola di Config	Linea guida
7.5.5	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
7,5,5	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.

ID controllo	AWS Regola di Config	Linea guida
7,5,7	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
7,5,7	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
7.5.7	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di Config	Linea guida
7.5.7	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
7.5.7	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	AWS Regola di Config	Linea guida
7.5.7	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
7.5.7	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	AWS Regola di Config	Linea guida
7,5,7	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di Config	Linea guida
7,5,7	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
7.5.7	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
7,5,7	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
7,5,7	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
8.1.1	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	AWS Regola di Config	Linea guida
8.1.1	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	AWS Regola di Config	Linea guida
8.1.1	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
8.1.1	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalen ti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di Config	Linea guida
8.1.1	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
8.1.1	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	AWS Regola di Config	Linea guida
8.1.1	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di Config	Linea guida
8.1.1	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibi le, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	AWS Regola di Config	Linea guida
8.1.2	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughpu t assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	AWS Regola di Config	Linea guida
8.1.2	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di Config	Linea guida
8.1.2	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
8.1.2	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) richiede almeno tre nodi di dati per un'elevata disponibilità e tolleranza ai guasti. L'implementazione di un dominio OpenSearch di servizio con almeno tre nodi di dati garantisce le operazioni del cluster in caso di guasto di un nodo.

ID controllo	AWS Regola di Config	Linea guida
8.1.2	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.
8.1.3	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	AWS Regola di Config	Linea guida
8.1.3	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individua re le possibili cause su cui indagare.
8.1.3	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatc h per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusi one dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
8.1.3	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
8.4.1	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	AWS Regola di Config	Linea guida
8.4.1	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
8.4.1	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	AWS Regola di Config	Linea guida
8.4.1	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
8.4.1	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiv a per le operazioni di I/O Amazon EBS. Tale ottimizza zione offre le prestazioni migliori in termini di efficienz a per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	AWS Regola di Config	Linea guida
8.4.1	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
8.4.1	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
8.4.1	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.
8.4.1	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatic i sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornalie ra. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazion e. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	AWS Regola di Config	Linea guida
8.4.1	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
8.4.1	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.

ID controllo	AWS Regola di Config	Linea guida
8.4.2	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
8.4.2	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
8.4.2	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
8.4.2	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
8.4.2	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
8.4.2	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
8.4.2	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.
8.4.2	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
8.4.2	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodica mente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.
8.4.2	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	AWS Regola di Config	Linea guida
8.4.2	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.
8.4.4	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
8,5,4	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di Config	Linea guida
8.5.4	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
91,1	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associa zione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.
9.1.1	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	AWS Regola di Config	Linea guida
9.1.1	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
9.1.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.1.1	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizza zioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
9.1.1	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.1.1	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.

ID controllo	AWS Regola di Config	Linea guida
9.1.1	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
9.1.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
9.1.1	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
9.1.1	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
9.1.1	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
9.1.1	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
9.1.1	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibili tà che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di Config	Linea guida
9.1.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.1.1	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
9.1.1	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
9.1.1	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
9.1.1	secretsmanager-rotation-ena bled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianifica zione regolare può abbreviar e il periodo di attività di un segreto e ridurre potenzial mente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	AWS Regola di Config	Linea guida
9.1.1	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
9.1.1	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	AWS Regola di Config	Linea guida
9.1.1	secretsmanager-secret-periodic-rotation	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione periodica abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto. Il valore predefinito è 90 giorni.
9.1.1	secretsmanager-secret-unused	Se in AWS Secrets Manager sono presenti credenziali inutilizzate, è necessario disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola consente di impostare un valore su unusedForDays (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.1.2	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.1.2	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizza zioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
9.1.2	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.1.2	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.
9.1.2	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
9.1.2	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
9.1.3	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
9.1.3	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatc h per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusi one dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
9.1.3	cloudtrail-enabled	AWS CloudTrail può contribui re a evitare il ripudio registran do le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizz ati in AWS CloudTrail Record Contents.
9.1.3	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrai l Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	AWS Regola di Config	Linea guida
9.1.3	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
9.1.3	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
9.1.3	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	AWS Regola di Config	Linea guida
9.1.3	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
9.1.3	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	AWS Regola di Config	Linea guida
9.1.3	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
9.1.3	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
9.1.3	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
9.1.3	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
9.1.3	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.1.3	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di Config	Linea guida
9.1.3	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
9.1.3	vpc-flow-logs-enabled	I log di flusso VPC forniscon o record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
9.1.3	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di Config	Linea guida
9.1.4	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
9.1.5	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
9.1.5	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
9.1.5	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
9.1.5	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
9.1.6	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.1.7	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
9.1.7	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.1.7	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizza zioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
9.1.7	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.1.7	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.
9.1.7	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
9.2.1	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
9.2.1	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
9.2.1	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
9.2.1	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
9.2.1	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di Config	Linea guida
9.2.1	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrai l Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
9.2.1	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzio ne dei problemi e le indagini forensi. La mancata disponibi lità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identif icazione di eventi potenzial mente dannosi.

ID controllo	AWS Regola di Config	Linea guida
9.2.1	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di Config	Linea guida
9.2.1	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
9.2.1	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.2.1	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
9.2.2	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
92,2	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
9.2.2	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
9.2.2	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di Config	Linea guida
9.2.2	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrai l Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
9.2.2	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzio ne dei problemi e le indagini forensi. La mancata disponibi lità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identif icazione di eventi potenzial mente dannosi.

ID controllo	AWS Regola di Config	Linea guida
92,2	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
9.2.2	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
9.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
9.2.2	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.2.2	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
9.3.1	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittogra fate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
9,31	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentir e ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
9,31	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
9.3.1	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
9.3.1	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
9.3.1	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS
9.3.1	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di Config	Linea guida
9.3.1	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
9.3.1	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
9,31	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	AWS Regola di Config	Linea guida
9.3.1	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
9.3.1	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
9,31	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
9.3.1	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
9.3.1	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
10.1.1	acm-certificate-expiration-check	Garantisci la protezion e dell'integrità della rete assicurando che i certifica ti X509 vengano emessi da ACM. AWS Questi certifica ti devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
10.1.1	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittogra fate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
10.1.1	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
10.1.1	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
10.1.1	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
10.1.1	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	AWS Regola di Config	Linea guida
10.1.1	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
10.1.1	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
10.1.1	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	AWS Regola di Config	Linea guida
10.1.1	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
10.1.1	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
10.1.1	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
10.1.1	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
10.1.1	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
10.1.1	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
10.1.1	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
10.1.1	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
10.1.1	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
10.1.1	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
10.1.1	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
10.1.1	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
10.1.1	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
10.1.1	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
10.1.1	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
10.1.1	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
10.1.1	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
10.1.1	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
10.1.1	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
10.1.1	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
10.2.1	acm-certificate-expiration-check	Garantisci la protezione e dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
10.2.1	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	AWS Regola di Config	Linea guida
10.2.1	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
10.2.2	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	AWS Regola di Config	Linea guida
10.2.3	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
10.2.3	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	AWS Regola di Config	Linea guida
10.2.3	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
11.1.1 (a)	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (a)	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
11.1.1 (a)	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
11.1.1 (a)	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (a)	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
11.1.1 (a)	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (a)	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
11.1.1 (a)	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
11.1.1 (a)	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (a)	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
11.1.1 (b)	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
11.1.1 (b)	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
11.1.1 (b)	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
11.1.1 (b)	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
11.1.1 (b)	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
11.1.1 (b)	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
11.1.1 (b)	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
11.1.1 (b)	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
11.1.1 (b)	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
11.1.1 (b)	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.
11.1.1 (b)	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
11.1.1 (b)	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.
11.1.1 (b)	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.
11.1.1 (b)	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
11.1.1 (b)	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
11.1.1 (b)	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
11.1.1 (b)	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
11.1.1 (b)	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
11.1.1 (b)	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
11.1.1 (b)	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
11.1.1 (b)	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
11.1.1 (b)	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
11.1.1 (b)	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
11.1.1 (b)	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.
11.1.1 (b)	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
11.1.1 (b)	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
11.1.1 (b)	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
11.1.3	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
11.1.3	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
11.1.3	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
11.1.3	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
11.1.3	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.
11.1.3	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
11.1.3	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
11.1.3	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenti cazione sono denominat i principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password e altre informazi oni amministrative su ogni principale.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizza zioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
11.1.3	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
11.1.3	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
11.1.3	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibili tà che un'identità riceva o mantenga privilegi eccessivi.
11.1.3	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
11.1.3	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
11.1.3	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
11.1.3	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di Config	Linea guida
11.1.3	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
11.1.3	s3-bucket-server-side-encry ption-enabled	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.
11.1.3	s3-default-encryption-kms	Assicurati che la crittogra fia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittogra fia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
11.1.3	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
11.1.3	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
11.1.3	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
11.2.1	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di Config	Linea guida
11.2.2	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
11.2.2	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
11.2.2	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
11.2.2	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
11.2.2	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di Config	Linea guida
11.2.2	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
11.2.2	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
11.2.2	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
11.2.2	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
11.2.2	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.
11.2.2	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
11.2.2	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
11.2.2	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
11.2.2	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
11.2.2	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
11.2.2	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
11.2.2	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
11.2.2	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
11.2.2	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
11.2.2	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
11.2.2	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	AWS Regola di Config	Linea guida
11.2.2	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
11.2.2	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di Config	Linea guida
11.2.2	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
11.2.4	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	AWS Regola di Config	Linea guida
11,2,4	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
11.2.4	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
11.2.4	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
11.2.4	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.
11.2.4	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
11.2.4	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
11.2.4	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
11.2.4	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	AWS Regola di Config	Linea guida
11.2.4	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.
11.2.4	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
11.2.4	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
11.2.4	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
11.2.4	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
11.2.4	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
11.2.4	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
11.2.4	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
11.2.4	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
11.2.4	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
11.2.4	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	AWS Regola di Config	Linea guida
11.2.4	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS
11.2.4	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di Config	Linea guida
11.3.1	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per protegger e l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
11.3.5	cloudtrail-enabled	AWS CloudTrail può contribui re a evitare il ripudio registran do le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizz ati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di Config	Linea guida
11.3.5	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
11.3.5	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
11.3.5	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
11.4.2	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
11.4.2	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.
11.4.2	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di Config	Linea guida
11.4.2	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.
11.5.2	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
12.1.1	cloudtrail-enabled	AWS CloudTrail può contribui re a evitare il ripudio registran do le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizz ati in AWS CloudTrail Record Contents.
12.1.1	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
12.1.1	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
12.1.1	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
12.2.2	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
122.2	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
12.2.2	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
12.2.2	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrai l Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	AWS Regola di Config	Linea guida
12.2.2	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
12.2.2	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
12.2.2	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	AWS Regola di Config	Linea guida
122.2	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
122.2	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
12.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
12.2.2	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
122.2	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
12.2.2	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di Config	Linea guida
122.2	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
12.2.2	vpc-flow-logs-enabled	I log di flusso VPC forniscon o record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di Config	Linea guida
122.2	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registraz ione WAF fornisce informazi oni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazi oni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
12.2.4	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
12.2.4	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
12.2.5	cloudtrail-enabled	AWS CloudTrail può contribui re a evitare il ripudio registran do le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizz ati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di Config	Linea guida
12.2.5	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
12.2.5	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
12.2.5	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
12.3.2	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di Config	Linea guida
12.3.2	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
12.3.2	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
14.1.2	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittogra fate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
14,1,2	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentir e ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
14,1,2	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
14.1.2	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
14.1.2	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
14.1.2	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
14,1,2	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
14.1.2	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
14,1,2	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
14,13	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
14.1.3	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consenton o, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	AWS Regola di Config	Linea guida
14.1.3	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
14.1.3	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
14.2.2	acm-certificate-expiration-check	Garantisci la protezion e dell'integrità della rete assicurando che i certifica ti X509 vengano emessi da ACM. AWS Questi certifica ti devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
14.2.2	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittogra fate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
142,2	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	AWS Regola di Config	Linea guida
142,2	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
142,2	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
14.2.2	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
142,2	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
142,2	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
14.2.2	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
14.2.2	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di Config	Linea guida
142,2	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
14.2.2	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.
14.2.6	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	AWS Regola di Config	Linea guida
14.2.6	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
14,2,6	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
14,2,6	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
14.2.6	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	AWS Regola di Config	Linea guida
14.2.6	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
14,2,6	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di Config	Linea guida
14,2,6	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for MAS TRMG.

Best practice operative per il monitoraggio

Questo pacchetto di conformità contiene AWS Config regole basate sul monitoraggio interno. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Monitoring.

Best practice operative per NBC TRMG

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il framework delle linee guida per la gestione dei rischi tecnologici (TRM) della National Bank of Cambodia (NBC) e le regole Config gestite. AWS Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a una o più linee guida NBC TRM. Una linea guida TRM NBC può essere correlata a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo modello di pacchetto di conformità di esempio contiene mappature ai controlli all'interno del framework delle linee guida del Technology Risk Management (TRM) della Banca Nazionale della Cambogia (NBC), a cui è possibile accedere qui: National Bank of Cambodia: Technology Risk Mangement Guidelines.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi.	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	- Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'effica ce segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisi one degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema,		sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	necessità che gli utenti effettivi abbiano l'accesso ed eliminazione di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'accesso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(d)	d) Tra i controlli importanti da considerare vi sono: - Un processo sistematico di applicazione e autorizzazione della creazione degli ID utente e della matrice di controllo degli accessi - L'esecuzione di una valutazione del rischio e la concessione dei diritti di accesso basati sugli stessi. - Implementazione del controllo degli accessi basato sui ruoli progettato per garantire un'efficace segregazione dei compiti - Modifica dei nomi utente e/o delle password predefiniti dei sistemi e divieto di condivisione degli ID utente e delle password degli account generici - Modifica dei diritti di accesso in caso di cambiamento di ruolo o responsabilità e	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	rimozione dei diritti di accesso in caso di cessazione del rapporto/contratto di lavoro - Processi per notificare tempestiv amente la funzione di sicurezza delle informazioni in merito alle aggiunte, alle eliminazioni e ai cambiamenti di ruolo degli utenti - Riconciliazione periodica degli ID utente in un sistema, necessità che gli utenti effettivi abbiano l'accesso ed eliminazi one di eventuali ID non necessari, se presenti - Audit, log e monitoraggio dell'acce sso agli asset IT da parte di tutti gli utenti e - Considerazione della disattivazione degli ID utente degli utenti di applicazioni critiche in congedo prolungato		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(f)	f) Ai fini della responsabilità, assicurati che gli utenti e gli asset IT siano identificati in modo univoco e che le relative azioni siano verificabili.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(f)	f) Ai fini della responsabilità, assicurati che gli utenti e gli asset IT siano identificati in modo univoco e che le relative azioni siano verificabili.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(f)	f) Ai fini della responsabilità, assicurati che gli utenti e gli asset IT siano identificati in modo univoco e che le relative azioni siano verificabili.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.
3.1.1(f)	f) Ai fini della responsabilità, assicurati che gli utenti e gli asset IT siano identificati in modo univoco e che le relative azioni siano verificabili.	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(f)	f) Ai fini della responsabilità, assicurati che gli utenti e gli asset IT siano identificati in modo univoco e che le relative azioni siano verificabili.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(f)	f) Ai fini della responsabilità, assicurati che gli utenti e gli asset IT siano identificati in modo univoco e che le relative azioni siano verificabili.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(f)	f) Ai fini della responsabilità, assicurati che gli utenti e gli asset IT siano identificati in modo univoco e che le relative azioni siano verificabili.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministr atori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabi lmente la capacità di infliggere gravi danni ai sistemi finanziar i che mantengon o o gestiscono in virtù delle funzioni lavorative e dell'acce sso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorveglia to e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenz e approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'accesso remoto da parte degli utenti con privilegi - Limitazione del numero di utenti con privilegi - Concessione dell'accesso privilegiato in base alle necessità o all'utilità - Mantenimento della registrazione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzione di audit periodici o revisione della gestione dei log - Divieto di condivisione degli ID con privilegi e dei relativi codici di accesso -		Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministr atori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabi lmente la capacità di infliggere gravi danni ai sistemi finanziar i che mantengon o o gestiscono in virtù delle funzioni lavorative e dell'acce sso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorveglia to e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenz e approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministr atori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabi lmente la capacità di infliggere gravi danni ai sistemi finanziar i che mantengon o o gestiscono in virtù delle funzioni lavorative e dell'acce sso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorveglia to e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenz e approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministr atori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabi lmente la capacità di infliggere gravi danni ai sistemi finanziar i che mantengon o o gestiscono in virtù delle funzioni lavorative e dell'acce sso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorveglia to e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenz e approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministr atori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabi lmente la capacità di infliggere gravi danni ai sistemi finanziar i che mantengon o o gestiscono in virtù delle funzioni lavorative e dell'acce sso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorveglia to e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenz e approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministr atori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabi lmente la capacità di infliggere gravi danni ai sistemi finanziar i che mantengon o o gestiscono in virtù delle funzioni lavorative e dell'acce sso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorveglia to e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenz e approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministr atori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabi lmente la capacità di infliggere gravi danni ai sistemi finanziar i che mantengon o o gestiscono in virtù delle funzioni lavorative e dell'acce sso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorveglia to e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenz e approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministr atori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabi lmente la capacità di infliggere gravi danni ai sistemi finanziar i che mantengon o o gestiscono in virtù delle funzioni lavorative e dell'acce sso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorveglia to e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenz e approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministr atori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabi lmente la capacità di infliggere gravi danni ai sistemi finanziar i che mantengon o o gestiscono in virtù delle funzioni lavorative e dell'acce sso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorveglia to e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenz e approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministratori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabilmente la capacità di infliggere gravi danni ai sistemi finanziari che mantengono o gestiscono in virtù delle funzioni lavorative e dell'accesso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorvegliato e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenze approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministr atori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabi lmente la capacità di infliggere gravi danni ai sistemi finanziar i che mantengon o o gestiscono in virtù delle funzioni lavorative e dell'acce sso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorveglia to e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenz e approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1(h)	h) Gli amministr atori di sistema, i responsabili della sicurezza, i programmatori e il personale che esegue operazioni critiche possiedono invariabi lmente la capacità di infliggere gravi danni ai sistemi finanziar i che mantengon o o gestiscono in virtù delle funzioni lavorative e dell'acce sso privilegiato. Il personale con elevati diritti di accesso al sistema deve essere strettamente sorveglia to e registrare tutte le attività relative ai sistemi, in quanto dispone di conoscenz e approfondite e degli asset necessari per aggirare i controlli dei sistemi e le procedure di sicurezza. È necessario prendere in considerazione alcune pratiche di controllo e sicurezza	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	elencate di seguito: - Implementazione dell'autenticazione a due fattori per gli utenti con privilegi - Istituzione di controlli rigorosi sull'acce sso remoto da parte degli utenti con privilegi - Limitazio ne del numero di utenti con privilegi - Concessione dell'acce sso privilegiato in base alle necessità o all'utilità - Mantenime nto della registraz ione di log di audit delle attività di sistema eseguite dagli utenti con privilegi - Garanzia che gli utenti con privilegi non abbiano accesso ai log di sistema in cui le attività vengono rilevate - Esecuzion e di audit periodici o revisione della gestione dei log - Divieto di condivisi one degli ID con privilegi e dei relativi codici di accesso -		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Impedire a fornitori e appaltatori di ottenere l'accesso con privilegi ai sistemi senza una stretta supervisione e monitoraggio e _ Protezione dei dati di backup da accessi non autorizzati		
3.1.2(a)	a) Il BFI deve installare dispositi vi di sicurezza di rete come firewall, software anti-viru s/anti-malware e sistemi di rilevamen to e prevenzione delle intrusioni nei punti critici della sua infrastruttura IT, per proteggere i perimetri di rete.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(a)	a) Il BFI deve installare dispositivi di sicurezza di rete come firewall, software anti-virus/anti-malware e sistemi di rilevamento e prevenzione delle intrusioni nei punti critici della sua infrastruttura IT, per proteggere i perimetri di rete.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(a)	a) Il BFI deve installare dispositivi di sicurezza di rete come firewall, software anti-virus/anti-malware e sistemi di rilevamento e prevenzione delle intrusioni nei punti critici della sua infrastruttura IT, per proteggere i perimetri di rete.	api-gw-associated-with-waf	AWS WAF consente di configurare una serie di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	acm-certificate-expiration-check	Garantisci che l'integrità della rete sia protetta assicurando che i certificati X509 siano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsab ilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e protegger e i sistemi e le applicazioni connessi (compresi i protocolli	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(c)	c) Devono essere implementati i controlli per garantire la sicurezza delle informazioni in rete e la protezione dei servizi connessi dall'accesso non autorizzato. In particolare, devono essere presi in considerazione i seguenti elementi: - Stabilire le responsabilità e le procedure per la gestione delle apparecchiature di rete - Separare la responsabilità operativa delle reti dalle operazioni informatiche, laddove opportuno - Stabilire controlli speciali per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni connessi (compresi i protocolli	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	di crittografia di rete) nel caso di connessio ne a sistemi/reti non affidabili. - È necessario applicare una registrazione e un monitoraggio adeguati per consentir e la registrazione e l'individuazione delle azioni che possono influire o sono rilevanti per la sicurezza delle informazi oni - Le attività di gestione devono essere strettamente coordinate sia per ottimizzare il servizio all'organizzazione sia per garantire che i controlli siano applicati in modo coerente in tutta l'infrastruttura di elaborazione delle informazioni - I sistemi sulla rete devono essere autenticati e - Le connessioni di sistema alla rete non affidabili devono essere limitate		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(e)	e) I servizi di rete possono variare dalla semplice larghezza di banda non gestita a servizi sofisticati come VPN, Voice over IP, VSAT, ecc. Le caratteristiche di sicurezza dei servizi di rete devono essere: - Tecnologia applicata per la sicurezza dei servizi di rete, come l'autenticazione, la crittografia e i controlli delle connessioni di rete - Parametri tecnici necessari per una connessione sicura ai servizi di rete in conformità alle regole di sicurezza e connessione alla rete e - Procedure per l'uso dei servizi di rete per limitare l'accesso ai servizi o alle applicazioni di rete, ove necessario	acm-certificate-expiration-check	Assicurati che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(e)	e) I servizi di rete possono variare dalla semplice larghezza di banda non gestita a servizi sofisticati come VPN, Voice over IP, VSAT, ecc. Le caratteristiche di sicurezza dei servizi di rete devono essere: - Tecnologia applicata per la sicurezza dei servizi di rete, come l'autenticazione, la crittografia e i controlli delle connessioni di rete - Parametri tecnici necessari per una connessione sicura ai servizi di rete in conformità alle regole di sicurezza e connessione alla rete e - Procedure per l'uso dei servizi di rete per limitare l'accesso ai servizi o alle applicazioni di rete, ove necessario	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(e)	e) I servizi di rete possono variare dalla semplice larghezza di banda non gestita a servizi sofisticati come VPN, Voice over IP, VSAT, ecc. Le caratteristiche di sicurezza dei servizi di rete devono essere: - Tecnologia applicata per la sicurezza dei servizi di rete, come l'autenticazione, la crittografia e i controlli delle connessioni di rete - Parametri tecnici necessari per una connessione sicura ai servizi di rete in conformità alle regole di sicurezza e connessione alla rete e - Procedure per l'uso dei servizi di rete per limitare l'accesso ai servizi o alle applicazioni di rete, ove necessario	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(e)	e) I servizi di rete possono variare dalla semplice larghezza di banda non gestita a servizi sofisticati come VPN, Voice over IP, VSAT, ecc. Le caratteristiche di sicurezza dei servizi di rete devono essere: - Tecnologia applicata per la sicurezza dei servizi di rete, come l'autenticazione, la crittografia e i controlli delle connessioni di rete - Parametri tecnici necessari per una connessione sicura ai servizi di rete in conformità alle regole di sicurezza e connessione alla rete e - Procedure per l'uso dei servizi di rete per limitare l'accesso ai servizi o alle applicazioni di rete, ove necessario	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(e)	e) I servizi di rete possono variare dalla semplice larghezza di banda non gestita a servizi sofisticati come VPN, Voice over IP, VSAT, ecc. Le caratteristiche di sicurezza dei servizi di rete devono essere: - Tecnologia applicata per la sicurezza dei servizi di rete, come l'autenticazione, la crittografia e i controlli delle connessioni di rete - Parametri tecnici necessari per una connessione sicura ai servizi di rete in conformità alle regole di sicurezza e connessione alla rete e - Procedure per l'uso dei servizi di rete per limitare l'accesso ai servizi o alle applicazioni di rete, ove necessario	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(e)	e) I servizi di rete possono variare dalla semplice larghezza di banda non gestita a servizi sofisticati come VPN, Voice over IP, VSAT, ecc. Le caratteristiche di sicurezza dei servizi di rete devono essere: - Tecnologia applicata per la sicurezza dei servizi di rete, come l'autenticazione, la crittografia e i controlli delle connessioni di rete - Parametri tecnici necessari per una connessione sicura ai servizi di rete in conformità alle regole di sicurezza e connessione alla rete e - Procedure per l'uso dei servizi di rete per limitare l'accesso ai servizi o alle applicazioni di rete, ove necessario	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(e)	e) I servizi di rete possono variare dalla semplice larghezza di banda non gestita a servizi sofisticati come VPN, Voice over IP, VSAT, ecc. Le caratteristiche di sicurezza dei servizi di rete devono essere: - Tecnologia applicata per la sicurezza dei servizi di rete, come l'autenticazione, la crittografia e i controlli delle connessioni di rete - Parametri tecnici necessari per una connessione sicura ai servizi di rete in conformità alle regole di sicurezza e connessione alla rete e - Procedure per l'uso dei servizi di rete per limitare l'accesso ai servizi o alle applicazioni di rete, ove necessario	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(e)	e) I servizi di rete possono variare dalla semplice larghezza di banda non gestita a servizi sofisticati come VPN, Voice over IP, VSAT, ecc. Le caratteristiche di sicurezza dei servizi di rete devono essere: - Tecnologia applicata per la sicurezza dei servizi di rete, come l'autenticazione, la crittografia e i controlli delle connessioni di rete - Parametri tecnici necessari per una connessione sicura ai servizi di rete in conformità alle regole di sicurezza e connessione alla rete e - Procedure per l'uso dei servizi di rete per limitare l'accesso ai servizi o alle applicazioni di rete, ove necessario	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(e)	e) I servizi di rete possono variare dalla semplice larghezza di banda non gestita a servizi sofisticati come VPN, Voice over IP, VSAT, ecc. Le caratteristiche di sicurezza dei servizi di rete devono essere: - Tecnologia applicata per la sicurezza dei servizi di rete, come l'autenticazione, la crittografia e i controlli delle connessioni di rete - Parametri tecnici necessari per una connessione sicura ai servizi di rete in conformità alle regole di sicurezza e connessione alla rete e - Procedure per l'uso dei servizi di rete per limitare l'accesso ai servizi o alle applicazioni di rete, ove necessario	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(e)	e) I servizi di rete possono variare dalla semplice larghezza di banda non gestita a servizi sofisticati come VPN, Voice over IP, VSAT, ecc. Le caratteristiche di sicurezza dei servizi di rete devono essere: - Tecnologia applicata per la sicurezza dei servizi di rete, come l'autenticazione, la crittografia e i controlli delle connessioni di rete - Parametri tecnici necessari per una connessione sicura ai servizi di rete in conformità alle regole di sicurezza e connessione alla rete e - Procedure per l'uso dei servizi di rete per limitare l'accesso ai servizi o alle applicazioni di rete, ove necessario	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2(e)	e) I servizi di rete possono variare dalla semplice larghezza di banda non gestita a servizi sofisticati come VPN, Voice over IP, VSAT, ecc. Le caratteristiche di sicurezza dei servizi di rete devono essere: - Tecnologia applicata per la sicurezza dei servizi di rete, come l'autenticazione, la crittografia e i controlli delle connessioni di rete - Parametri tecnici necessari per una connessione sicura ai servizi di rete in conformità alle regole di sicurezza e connessione alla rete e - Procedure per l'uso dei servizi di rete per limitare l'accesso ai servizi o alle applicazioni di rete, ove necessario	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(e)	e) Utilizza la crittografia per proteggere i canali di comunicazione tra il dispositivo di accesso remoto e l'ente per limitare i rischi legati allo spoofing di rete.	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
3.1.3(e)	e) Utilizza la crittografia per proteggere i canali di comunicazione tra il dispositivo di accesso remoto e l'ente per limitare i rischi legati allo spoofing di rete.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(e)	e) Utilizza la crittografia per proteggere i canali di comunicazione tra il dispositivo di accesso remoto e l'ente per limitare i rischi legati allo spoofing di rete.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
3.1.3(e)	e) Utilizza la crittografia per proteggere i canali di comunicazione tra il dispositivo di accesso remoto e l'ente per limitare i rischi legati allo spoofing di rete.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(e)	e) Utilizza la crittografia per proteggere i canali di comunicazione tra il dispositivo di accesso remoto e l'ente per limitare i rischi legati allo spoofing di rete.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.1.3(e)	e) Utilizza la crittografia per proteggere i canali di comunicazione tra il dispositivo di accesso remoto e l'ente per limitare i rischi legati allo spoofing di rete.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(e)	e) Utilizza la crittografia per proteggere i canali di comunicazione tra il dispositivo di accesso remoto e l'ente per limitare i rischi legati allo spoofing di rete.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(e)	e) Utilizza la crittografia per proteggere i canali di comunicazione tra il dispositivo di accesso remoto e l'ente per limitare i rischi legati allo spoofing di rete.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.1.3(e)	e) Utilizza la crittografia per proteggere i canali di comunicazione tra il dispositivo di accesso remoto e l'ente per limitare i rischi legati allo spoofing di rete.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(e)	e) Utilizza la crittografia per proteggere i canali di comunicazione tra il dispositivo di accesso remoto e l'ente per limitare i rischi legati allo spoofing di rete.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
3.1.3(e)	e) Utilizza la crittografia per proteggere i canali di comunicazione tra il dispositivo di accesso remoto e l'ente per limitare i rischi legati allo spoofing di rete.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(g)	g) Conserva i log per le comunicazioni di accesso remoto. I log devono includere la data, l'ora, l'utente, la posizione dell'utente, la durata e lo scopo di tutti gli accessi remoti, comprese tutte le attività svolte tramite accesso remoto	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(i)	i) Applica il processo di autenticazione a due fattori per l'accesso remoto (ad esempio, scheda token basata su PIN con generatore di password casuali monouso o PKI basata su token)	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel Cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(i)	i) Applica il processo di autenticazione a due fattori per l'accesso remoto (ad esempio, token card basata su PIN con generatore di password casuali monouso o PKI basata su token)	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(i)	i) Applica il processo di autenticazione a due fattori per l'accesso remoto (ad esempio, scheda token basata su PIN con generatore di password casuali monouso o PKI basata su token)	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3(i)	i) Implementazione del processo di autenticazione a due fattori per l'accesso remoto (ad esempio, scheda token basata su PIN con generatore di password casuali monouso o PKI basata su token)	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4(c)(e)	c) Il processo di gestione delle patch dovrebbe includere aspetti quali: - Determinazione dei metodi per ottenere e convalidare le patch per garantire che la patch provenga da una fonte autorizzata - Identificazione delle vulnerabilità applicabili alle applicazioni e ai sistemi utilizzati dall'organizzazione e - Valutazione dell'impatto aziendale dell'implementazione delle patch (o della mancata implementazione di una particolare patch) - Garantire che le patch siano testate - Descrivere i metodi per distribuire le patch, ad esempio automaticamente - Rapporti sullo stato della distribuzione delle patch in tutta l'organizzazione e - Metodi inclusi per	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	gestire l'implementazione non riuscita di una patch (ad esempio, la ridistribuzione della patch). e) I BFI dovrebbero implementare strumenti automatici di gestione delle patch e strumenti di aggiornamento software per tutti i sistemi per i quali tali strumenti sono disponibili e sicuri		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4(c)(e)	c) Il processo di gestione delle patch dovrebbe includere aspetti quali: - Determinazione dei metodi per ottenere e convalidare le patch per garantire che la patch provenga da una fonte autorizzata - Identificazione delle vulnerabilità applicabili alle applicazioni e ai sistemi utilizzati dall'organizzazione - Valutazione dell'impatto aziendale dell'implementazione delle patch (o della mancata implementazione di una particolare patch) - Garantire che le patch siano testate - Descrivere i metodi per distribuire le patch, ad esempio automaticamente - Rapporti sullo stato della distribuzione delle patch in tutta l'organizzazione e - Metodi inclusi per	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	gestire l'implementazione non riuscita di una patch (ad esempio, la ridistribuzione della patch). e) I BFI dovrebbero implementare strumenti automatici di gestione delle patch e strumenti di aggiornamento software per tutti i sistemi per i quali tali strumenti sono disponibili e sicuri		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4(c)(e)	c) Il processo di gestione delle patch dovrebbe includere aspetti quali: - Determinazione dei metodi per ottenere e convalidare le patch per garantire che la patch provenga da una fonte autorizzata - Identificazione delle vulnerabilità applicabili alle applicazioni e ai sistemi utilizzati dall'organizzazione - Valutazione dell'impatto aziendale dell'implementazione delle patch (o della mancata implementazione di una particolare patch) - Garantire che le patch siano testate - Descrivere i metodi per distribuire le patch, ad esempio automaticamente - Rapporti sullo stato della distribuzione delle patch in tutta l'organizzazione e - Metodi inclusi per	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	gestire l'implementazione non riuscita di una patch (ad esempio, la ridistribuzione della patch). e) I BFI dovrebbero implementare strumenti automatici di gestione delle patch e strumenti di aggiornamento software per tutti i sistemi per i quali tali strumenti sono disponibili e sicuri		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4(c)(e)	c) Il processo di gestione delle patch dovrebbe includere aspetti quali: - Determinazione dei metodi per ottenere e convalidare le patch per garantire che la patch provenga da una fonte autorizzata - Identificazione delle vulnerabilità applicabili alle applicazioni e ai sistemi utilizzati dall'organizzazione - Valutazione dell'impatto aziendale dell'implementazione delle patch (o della mancata implementazione di una particolare patch) - Garantire che le patch siano testate - Descrivere i metodi per distribuire le patch, ad esempio automaticamente - Rapporti sullo stato della distribuzione delle patch in tutta l'organizzazione e - Metodi inclusi per	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	gestire l'implementazione non riuscita di una patch (ad esempio, la ridistribuzione della patch). e) I BFI dovrebbero implementare strumenti automatici di gestione delle patch e strumenti di aggiornamento software per tutti i sistemi per i quali tali strumenti sono disponibili e sicuri		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4(c)(e)	c) Il processo di gestione delle patch dovrebbe includere aspetti quali: - Determinazione dei metodi per ottenere e convalidare le patch per garantire che la patch provenga da una fonte autorizzata - Identificazione delle vulnerabilità applicabili alle applicazioni e ai sistemi utilizzati dall'organizzazione - Valutazione dell'impatto aziendale dell'implementazione delle patch (o della mancata implementazione di una particolare patch) - Garantire che le patch siano testate - Descrivere i metodi per distribuire le patch, ad esempio automaticamente - Rapporti sullo stato della distribuzione delle patch in tutta l'organizzazione e - Metodi inclusi per	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	gestire l'implementazione non riuscita di una patch (ad esempio, la ridistribuzione della patch). e) I BFI dovrebbero implementare strumenti automatici di gestione delle patch e strumenti di aggiornamento software per tutti i sistemi per i quali tali strumenti sono disponibili e sicuri		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4(c)(e)	c) Il processo di gestione delle patch dovrebbe includere aspetti quali: - Determinazione dei metodi per ottenere e convalidare le patch per garantire che la patch provenga da una fonte autorizzata - Identificazione delle vulnerabilità applicabili alle applicazioni e ai sistemi utilizzati dall'organizzazione e - Valutazione dell'impatto aziendale dell'implementazione delle patch (o della mancata implementazione di una particolare patch) - Garantire che le patch siano testate - Descrivere i metodi per distribuire le patch, ad esempio automaticamente - Rapporti sullo stato della distribuzione delle patch in tutta l'organizzazione e - Metodi inclusi per	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	gestire l'implementazione non riuscita di una patch (ad esempio, la ridistribuzione della patch). e) I BFI dovrebbero implementare strumenti automatici di gestione delle patch e strumenti di aggiornamento software per tutti i sistemi per i quali tali strumenti sono disponibili e sicuri		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5(d)(e)	d) Un'adeguata gestione delle chiavi richiede processi sicuri per la generazione, l'archiviazione, il recupero, la distribuzione, il ritiro e la distruzione delle chiavi crittografiche e) Tutte le chiavi crittografiche devono essere protette da modifiche e perdite. Inoltre, le chiavi segrete e private devono essere protette dall'uso non autorizzato e dalla divulgazione. Le apparecchiature utilizzate per generare, conservare e archiviare le chiavi devono essere protette fisicamente	kms-cmk-not-scheduled-for-deletion	Per contribuire a proteggere i dati archiviati, assicuratevi che non sia pianificata l'eliminazione delle chiavi master dei clienti (CMK) necessarie nel AWS Key Management Service (KMS).AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5(d)(e)	d) Un'adeguata gestione delle chiavi richiede processi sicuri per la generazione, l'archiviazione, il recupero, la distribuzione, il ritiro e la distruzione delle chiavi crittografiche e) Tutte le chiavi crittografiche devono essere protette da modifiche e perdite. Inoltre, le chiavi segrete e private devono essere protette dall'uso non autorizzato e dalla divulgazione. Le apparecchiature utilizzate per generare, conservare e archiviare le chiavi devono essere protette fisicamente	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5(d)(e)	d) Un'adeguata gestione delle chiavi richiede processi sicuri per la generazione, l'archiviazione, il recupero, la distribuzione, il ritiro e la distruzione delle chiavi crittografiche e) Tutte le chiavi crittografiche devono essere protette da modifiche e perdite. Inoltre, le chiavi segrete e private devono essere protette dall'uso non autorizzato e dalla divulgazione. Le apparecchiature utilizzate per generare, conservare e archiviare le chiavi devono essere protette fisicamente	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5(d)(e)	d) Un'adeguata gestione delle chiavi richiede processi sicuri per la generazione, l'archiviazione, il recupero, la distribuzione, il ritiro e la distruzione delle chiavi crittografiche e) Tutte le chiavi crittografiche devono essere protette da modifiche e perdite. Inoltre, le chiavi segrete e private devono essere protette dall'uso non autorizzato e dalla divulgazione. Le apparecchiature utilizzate per generare, conservare e archiviare le chiavi devono essere protette fisicamente	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5(f)	f) Un sistema di gestione delle chiavi dovrebbe basarsi su un insieme concordato di standard, procedure e metodi sicuri per: - generare chiavi per diversi sistemi crittografici e diverse applicazioni - emettere e ottenere certificati a chiave pubblica - distribuire le chiavi alle entità previste, incluso il modo in cui le chiavi devono essere attivate al momento della ricezione - archiviare le chiavi, incluso il modo in cui gli utenti autorizzati ottengono l'accesso alle chiavi - modificare o aggiornare le chiavi, comprese le regole su quando cambiare le chiavi e come farlo - gestire le chiavi compromesse - revoca delle chiavi, comprese le chiavi how devono essere	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che le chiavi master del cliente (CMK) necessarie non siano pianificate per l'eliminazione in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ritirate o disattivate, ad esempio quando le chiavi sono state compromesse o quando un utente lascia un'organizzazione (nel qual caso anche le chiavi devono essere archiviate) - recuperare le chiavi perse o danneggiate - eseguire il backup o l'archiviazione delle chiavi - distruggere le chiavi e - registrare e controllare le attività relative alla gestione delle chiavi.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5(f)	f) Un sistema di gestione delle chiavi dovrebbe basarsi su un insieme concordato di standard, procedure e metodi sicuri per: - generare chiavi per diversi sistemi crittografici e diverse applicazioni - emettere e ottenere certificati a chiave pubblica - distribuire le chiavi alle entità previste, incluso il modo in cui le chiavi devono essere attivate al momento della ricezione - archiviare le chiavi, incluso il modo in cui gli utenti autorizzati ottengono l'accesso alle chiavi - modificare o aggiornare le chiavi, comprese le regole su quando cambiare le chiavi e come farlo - gestire le chiavi compromesse - revoca delle chiavi, comprese le chiavi how devono essere	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che vengano ruotate dopo che hanno raggiunto la fine del loro periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ritirate o disattivate, ad esempio quando le chiavi sono state compromesse o quando un utente lascia un'organi zzazione (nel qual caso anche le chiavi devono essere archiviate) - recuperar e le chiavi perse o danneggiate - eseguire il backup o l'archiviazione delle chiavi - distruggere le chiavi e - registrare e controllare le attività relative alla gestione delle chiavi.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5(f)	f) Un sistema di gestione delle chiavi dovrebbe basarsi su un insieme concordato di standard, procedure e metodi sicuri per: - generare chiavi per diversi sistemi crittografici e diverse applicazioni - emettere e ottenere certificati a chiave pubblica - distribuire le chiavi alle entità previste, incluso il modo in cui le chiavi devono essere attivate al momento della ricezione - archiviare le chiavi, incluso il modo in cui gli utenti autorizzati ottengono l'accesso alle chiavi - modificare o aggiornare le chiavi, comprese le regole su quando cambiare le chiavi e come farlo - gestire le chiavi compromesse - revoca delle chiavi, comprese le chiavi how devono essere	acm-certificate-expiration-check	Assicurati che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ritirate o disattivate, ad esempio quando le chiavi sono state compromesse o quando un utente lascia un'organizzazione (nel qual caso anche le chiavi devono essere archiviate) - recuperare le chiavi perse o danneggiate - eseguire il backup o l'archiviazione delle chiavi - distruggere le chiavi e - registrare e controllare le attività relative alla gestione delle chiavi.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5(f)	f) Un sistema di gestione delle chiavi dovrebbe basarsi su un insieme concordato di standard, procedure e metodi sicuri per: - generare chiavi per diversi sistemi crittografici e diverse applicazioni - emettere e ottenere certificati a chiave pubblica - distribuire le chiavi alle entità previste, incluso il modo in cui le chiavi devono essere attivate al momento della ricezione - archiviare le chiavi, incluso il modo in cui gli utenti autorizzati ottengono l'accesso alle chiavi - modificare o aggiornare le chiavi, comprese le regole su quando cambiare le chiavi e come farlo - gestire le chiavi compromesse - revoca delle chiavi, comprese le chiavi how devono essere	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ritirate o disattivate, ad esempio quando le chiavi sono state compromesse o quando un utente lascia un'organi zzazione (nel qual caso anche le chiavi devono essere archiviate) - recuperar e le chiavi perse o danneggiate - eseguire il backup o l'archiviazione delle chiavi - distruggere le chiavi e - registrare e controllare le attività relative alla gestione delle chiavi.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5(f)	f) Un sistema di gestione delle chiavi dovrebbe basarsi su un insieme concordato di standard, procedure e metodi sicuri per: - generare chiavi per diversi sistemi crittografici e diverse applicazioni - emettere e ottenere certificati a chiave pubblica - distribuire le chiavi alle entità previste, incluso il modo in cui le chiavi devono essere attivate al momento della ricezione - archiviare le chiavi, incluso il modo in cui gli utenti autorizzati ottengono l'accesso alle chiavi - modificare o aggiornare le chiavi, comprese le regole su quando cambiare le chiavi e come farlo - gestire le chiavi compromesse - revoca delle chiavi, comprese le chiavi how devono essere	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di gestione e le chiamate API. AWS È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ritirate o disattivate, ad esempio quando le chiavi sono state compromesse o quando un utente lascia un'organizzazione (nel qual caso anche le chiavi devono essere archiviate) - recuperare le chiavi perse o danneggiate - eseguire il backup o l'archiviazione delle chiavi - distruggere le chiavi e - registrare e controllare le attività relative alla gestione delle chiavi.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5(f)	f) Un sistema di gestione delle chiavi dovrebbe basarsi su un insieme concordato di standard, procedure e metodi sicuri per: - generare chiavi per diversi sistemi crittografici e diverse applicazioni - emettere e ottenere certificati a chiave pubblica - distribuire le chiavi alle entità previste, incluso il modo in cui le chiavi devono essere attivate al momento della ricezione - archiviare le chiavi, incluso il modo in cui gli utenti autorizzati ottengono l'accesso alle chiavi - modificare o aggiornare le chiavi, comprese le regole su quando cambiare le chiavi e come farlo - gestire le chiavi compromesse - revoca delle chiavi, comprese le chiavi how devono essere	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di gestione e le chiamate API. AWS È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ritirate o disattivate, ad esempio quando le chiavi sono state compromesse o quando un utente lascia un'organizzazione (nel qual caso anche le chiavi devono essere archiviate) - recuperare le chiavi perse o danneggiate - eseguire il backup o l'archiviazione delle chiavi - distruggere le chiavi e - registrare e controllare le attività relative alla gestione delle chiavi.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5(f)	f) Un sistema di gestione delle chiavi dovrebbe basarsi su un insieme concordato di standard, procedure e metodi sicuri per: - generare chiavi per diversi sistemi crittografici e diverse applicazioni - emettere e ottenere certificati a chiave pubblica - distribuire le chiavi alle entità previste, incluso il modo in cui le chiavi devono essere attivate al momento della ricezione - archiviare le chiavi, incluso il modo in cui gli utenti autorizzati ottengono l'accesso alle chiavi - modificare o aggiornare le chiavi, comprese le regole su quando cambiare le chiavi e come farlo - gestire le chiavi compromesse - revoca delle chiavi, comprese le chiavi how devono essere	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	ritirate o disattivate, ad esempio quando le chiavi sono state compromesse o quando un utente lascia un'organizzazione (nel qual caso anche le chiavi devono essere archiviate) - recuperare le chiavi perse o danneggiate - eseguire il backup o l'archiviazione delle chiavi - distruggere le chiavi e - registrare e controllare le attività relative alla gestione delle chiavi.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.6(a)	a) Il BFI deve utilizzare una combinazione di strumenti automatizzati e tecniche manuali per eseguire una VA completa su base periodica. Per i sistemi con interfaccia esterna basati sul Web, l'ambito della VA deve includere le vulnerabilità Web comuni, come l'iniezione SQL e lo scripting tra siti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.6(a)	a) Il BFI deve utilizzare una combinazione di strumenti automatizzati e tecniche manuali per eseguire una VA completa su base periodica. Per i sistemi con interfaccia esterna basati sul Web, l'ambito della VA deve includere le vulnerabilità Web comuni, come l'iniezione SQL e lo scripting tra siti.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.6(a)	a) Il BFI deve utilizzare una combinazione di strumenti automatizzati e tecniche manuali per eseguire una VA completa su base periodica. Per i sistemi con interfaccia esterna basati sul Web, l'ambito della VA deve includere le vulnerabilità Web comuni, come l'iniezione SQL e lo scripting tra siti.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
3.1.6(c)	c) Il BFI deve stabilire un processo per porre rimedio ai problemi identificati nella VA e nel PT ed eseguire una successiva riconvalida della correzione per verificare che le lacune siano state completamente colmate.	vuln-mitigated-accepted(controllo di processo)	Assicurati che le vulnerabilità appena identificate vengano corrette o documentate come rischi accettati. Le vulnerabilità devono essere corrette o accettate come rischi in base ai requisiti di conformità dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.6(f)	f) Su base periodica , la funzione di sicurezza deve fornire alla dirigenza senior gli aggiornamenti sullo stato di avanzamento per quanto riguarda il numero di vulnerabi lità critiche e non mitigate, per ciascun reparto/divisione, e un piano per la mitigazio ne	guardduty-non-arch ived-findings	Amazon ti GuardDuty aiuta a comprende re l'impatto di un incidente classific ando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltati vamente daysLowSe v (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviat i, come richiesto dalle politiche dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.8	Formazione e consapevolezza degli utenti	security-awareness -program-exists (controllo di processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organiz zazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili come la documentazione del sistema, il codice sorgente dell'appl icazione e i dati delle transazioni di produzione dovrebber o essere oggetto di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuz ione di informazioni sensibili, comprese le stampe che le contengono.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili come la documentazione del sistema, il codice sorgente dell'appl icazione e i dati delle transazioni di produzione dovrebber o essere oggetto di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuz ione di informazioni sensibili, comprese le stampe che le contengono.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili come la documentazione del sistema, il codice sorgente dell'applicazione e i dati delle transazioni di produzione dovrebbero essere oggetto di controlli più estesi per prevenire eventuali alterazioni (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuzione di informazioni sensibili, comprese le stampe che le contengono.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili come la documentazione del sistema, il codice sorgente dell'appl icazione e i dati delle transazioni di produzione dovrebber o essere oggetto di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuz ione di informazioni sensibili, comprese le stampe che le contengono.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili, come la documentazione del sistema, il codice sorgente dell'applicazione e i dati delle transazioni di produzione, dovrebbero essere dotate di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuzione di informazioni sensibili, comprese le stampe che le contengono.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili come la documentazione del sistema, il codice sorgente dell'applicazione e i dati delle transazioni di produzione dovrebbero essere dotate di controlli più estesi per prevenire eventuali alterazioni (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuzione di informazioni sensibili, comprese le stampe che le contengono.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili come la documentazione del sistema, il codice sorgente dell'appl icazione e i dati delle transazioni di produzione dovrebber o essere oggetto di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuz ione di informazioni sensibili, comprese le stampe che le contengono.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili, come la documentazione del sistema, il codice sorgente dell'appl icazione e i dati delle transazio ni di produzione, dovrebbero essere dotate di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuz ione di informazioni sensibili, comprese le stampe che le contengono.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili, come la documentazione del sistema, il codice sorgente dell'applicazione e i dati delle transazioni di produzione, dovrebbero essere dotate di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuzione di informazioni sensibili, comprese le stampe che le contengono.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili come la documentazione del sistema, il codice sorgente dell'appl icazione e i dati delle transazio ni di produzione dovrebbero essere dotate di controlli più estesi per prevenire eventuali alterazioni (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuz ione di informazioni sensibili, comprese le stampe che le contengono.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili, come la documentazione del sistema, il codice sorgente dell'applicazione e i dati delle transazioni di produzione, dovrebbero essere dotate di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuzione di informazioni sensibili, comprese le stampe che le contengono.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili, come la documentazione del sistema, il codice sorgente dell'appl icazione e i dati delle transazio ni di produzione, dovrebbero essere dotate di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuz ione di informazioni sensibili, comprese le stampe che le contengono.	sagemaker-notebook -instance-kms-key- configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili come la documentazione del sistema, il codice sorgente dell'applicazione e i dati delle transazioni di produzione dovrebbero essere oggetto di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuzione di informazioni sensibili, comprese le stampe che le contengono.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili, come la documentazione del sistema, il codice sorgente dell'appl icazione e i dati delle transazio ni di produzione, dovrebbero essere soggette a controlli più approfonditi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuz ione di informazioni sensibili, comprese le stampe che le contengono.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili, come la documentazione del sistema, il codice sorgente dell'applicazione e i dati delle transazioni di produzione, dovrebbero essere dotate di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuzione di informazioni sensibili, comprese le stampe che le contengono.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili, come la documentazione del sistema, il codice sorgente dell'appl icazione e i dati delle transazio ni di produzione, dovrebbero essere dotate di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuz ione di informazioni sensibili, comprese le stampe che le contengono.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili, come la documentazione del sistema, il codice sorgente dell'applicazione e i dati delle transazioni di produzione, dovrebbero essere dotate di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuzione di informazioni sensibili, comprese le stampe che le contengono.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili, come la documentazione del sistema, il codice sorgente dell'applicazione e i dati delle transazioni di produzione, dovrebbero essere dotate di controlli più estesi per evitarne l'alterazione (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuzione di informazioni sensibili, comprese le stampe che le contengono.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili, come la documentazione del sistema, il codice sorgente dell'appl icazione e i dati delle transazio ni di produzione, dovrebbero essere sottoposte a controlli più approfonditi per prevenire eventuali alterazioni (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuz ione di informazioni sensibili, comprese le stampe che le contengono.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.10(b)	b) Le informazioni sensibili come la documentazione del sistema, il codice sorgente dell'applicazione e i dati delle transazioni di produzione dovrebbero essere dotate di controlli più estesi per prevenire eventuali alterazioni (ad esempio, controlli di integrità, hash crittografici). Inoltre, le policy devono ridurre al minimo la distribuzione di informazioni sensibili, comprese le stampe che le contengono.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(h)	h) Per ridurre al minimo i rischi associati alle modifiche, le BFI devono eseguire il backup dei sistemi o delle applicazioni interessati prima di eventuali modifiche . Le BFI devono stabilire un piano di rollback per ripristin are una versione precedente del sistema o dell'appl icazione se si verifica un problema durante o dopo l'impleme ntazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(h)	h) Per ridurre al minimo i rischi associati alle modifiche, le BFI devono eseguire il backup dei sistemi o delle applicazioni interessati prima di eventuali modifiche . Le BFI devono stabilire un piano di rollback per ripristin are una versione precedente del sistema o dell'appl icazione se si verifica un problema durante o dopo l'impleme ntazione.	dynamodb-pitr-enab led	Abilita questa regola per verificare che sia stato eseguito il backup delle informazi oni. Inoltre, mantiene i backup assicuran do che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristin o mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(h)	h) Per ridurre al minimo i rischi associati alle modifiche, le BFI devono eseguire il backup dei sistemi o delle applicazioni interessati prima di eventuali modifiche. Le BFI devono stabilire un piano di rollback per ripristinare una versione precedente del sistema o dell'applicazione se si verifica un problema durante o dopo l'implementazione.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(h)	h) Per ridurre al minimo i rischi associati alle modifiche, le BFI devono eseguire il backup dei sistemi o delle applicazioni interessati prima di eventuali modifiche . Le BFI devono stabilire un piano di rollback per ripristin are una versione precedente del sistema o dell'appl icazione se si verifica un problema durante o dopo l'impleme ntazione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(h)	h) Per ridurre al minimo i rischi associati alle modifiche, le BFI devono eseguire il backup dei sistemi o delle applicazioni interessati prima di eventuali modifiche . Le BFI devono stabilire un piano di rollback per ripristin are una versione precedente del sistema o dell'appl icazione se si verifica un problema durante o dopo l'impleme ntazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(h)	h) Per ridurre al minimo i rischi associati alle modifiche, le BFI devono eseguire il backup dei sistemi o delle applicazioni interessati prima di eventuali modifiche . Le BFI devono stabilire un piano di rollback per ripristin are una versione precedente del sistema o dell'appl icazione se si verifica un problema durante o dopo l'impleme ntazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(h)	h) Per ridurre al minimo i rischi associati alle modifiche, le BFI devono eseguire il backup dei sistemi o delle applicazioni interessati prima di eventuali modifiche . Le BFI devono stabilire un piano di rollback per ripristin are una versione precedente del sistema o dell'appl icazione se si verifica un problema durante o dopo l'impleme ntazione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(h)	h) Per ridurre al minimo i rischi associati alle modifiche, le BFI devono eseguire il backup dei sistemi o delle applicazioni interessati prima di eventuali modifiche . Le BFI devono stabilire un piano di rollback per ripristin are una versione precedente del sistema o dell'appl icazione se si verifica un problema durante o dopo l'impleme ntazione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(h)	h) Per ridurre al minimo i rischi associati alle modifiche, le BFI devono eseguire il backup dei sistemi o delle applicazioni interessati prima di eventuali modifiche . Le BFI devono stabilire un piano di rollback per ripristin are una versione precedente del sistema o dell'appl icazione se si verifica un problema durante o dopo l'impleme ntazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(h)	h) Per ridurre al minimo i rischi associati alle modifiche, le BFI devono eseguire il backup dei sistemi o delle applicazioni interessati prima di eventuali modifiche . Le BFI devono stabilire un piano di rollback per ripristin are una versione precedente del sistema o dell'appl icazione se si verifica un problema durante o dopo l'impleme ntazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(h)	h) Per ridurre al minimo i rischi associati alle modifiche, le BFI devono eseguire il backup dei sistemi o delle applicazioni interessati prima di eventuali modifiche . Le BFI devono stabilire un piano di rollback per ripristin are una versione precedente del sistema o dell'appl icazione se si verifica un problema durante o dopo l'impleme ntazione.	redshift-backup-en abled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatiz zati. Quando gli snapshot automatic i sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazi one predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazion e.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazion e.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazione.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazione.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazione.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazione.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1(k)	k) I log di controllo e sicurezza sono informazioni utili che facilitano le indagini e la risoluzione dei problemi. Il BFI deve garantire che l'utilità di log sia abilitata a registrare le attività eseguite durante il processo di migrazione.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.3(a)	a) Sviluppa e implementa processi per prevenire, rilevare, analizzar e e rispondere agli incidenti di sicurezza delle informazioni.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.3(a)	a) Sviluppa e implementa processi per prevenire, rilevare, analizzar e e rispondere agli incidenti di sicurezza delle informazioni.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
3.3.1(a)	a) Considerare i fattori importanti associati al mantenimento dell'elevata disponibilità del sistema, della capacità adeguata, dell'affidabilità delle prestazioni, dei tempi di risposta rapidi e della scalabilità come parte della progettazione del sistema.	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(a)(b)(c)(f)(j)	a) Garantire che le registrazioni degli accessi degli utenti siano identificate e registrate in modo univoco ai fini di controllo e revisione . b) Documentare la responsabilità e l'identificazione degli accessi non autorizzati. c) Abilitare il logging di controllo delle attività di sistema eseguite da utenti con privilegi . f) Garantire che la registrazione e il monitoraggio siano appropriati per consentire il logging e il rilevamento di azioni che possono influire o siano rilevanti per la sicurezza delle informazioni. j) Garantire che il logging e il monitoraggio siano appropriati per consentire la registrazione e il rilevamento di azioni che possono	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	influire o sono rilevanti per la sicurezza delle informazioni. j) Garantire che la registrazione e il monitoraggio siano sistemi appropriati in grado di generare report e avvisi consolidati sulla sicurezza del sistema.		
3.4(f)	f) Assicurarsi che vengano applicati il logging e il monitoraggio appropriati per consentire la registrazione e il rilevamento di azioni che possono influire o sono rilevanti per la sicurezza delle informazioni.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identific atore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registraz ioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazi oni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identificatore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registrazioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazioni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identific atore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registraz ioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazi oni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identific atore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registraz ioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazi oni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identificatore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registrazioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazioni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identificatore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registrazioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazioni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identificatore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registrazioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazioni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identificatore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registrazioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazioni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identificatore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registrazioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazioni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identific atore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registraz ioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazi oni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identific atore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registraz ioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazi oni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identificatore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registrazioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazioni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identificatore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registrazioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazioni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4(g)	g) Assicurarsi che i registri degli eventi includano, se pertinente: - ID utente - Attività di sistema - Date, ora e dettagli degli eventi chiave, ad esempio accesso e disconnessione - Identità o posizione del dispositivo, se possibile, e identificatore del sistema - Registrazioni dei tentativi di accesso al sistema riusciti e rifiutati - Registrazioni dei dati riusciti e rifiutati e altri tentativi di accesso alle risorse - Modifiche alla configurazione del sistema - Uso dei privilegi - Uso delle utilità e delle applicazioni di sistema - File a cui si accede e tipo di accesso - Indirizzi e protocolli di rete - Allarmi generati dal sistema di controllo degli accessi e - Registrazioni delle	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	transazioni eseguite dagli utenti nelle applicazioni e delle transazioni online con i clienti		
3.6.1(a)(h)	a) Le BFI devono garantire misure di sicurezza adeguate per le applicazi oni web e adottare misure di mitigazio ne ragionevoli contro diversi rischi per la sicurezza del web. h) Le BFI devono garantire misure di sicurezza adeguate per le applicazi oni web e adottare misure di mitigazio ne ragionevoli contro diversi rischi per la sicurezza del Web	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(a)(h)	a) Le BFI devono garantire misure di sicurezza adeguate per le applicazi oni web e adottare misure di mitigazio ne ragionevoli contro diversi rischi per la sicurezza del web. h) Le BFI devono garantire misure di sicurezza adeguate per le applicazi oni web e adottare misure di mitigazio ne ragionevoli contro diversi rischi per la sicurezza del Web	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(b)	b) Le BFI devono valutare i requisiti di sicurezza associati ai loro sistemi di internet banking e ad altri sistemi pertinenti e adottare una soluzione di crittografia che tenga conto del grado di riservatezza e integrità richiesto.	acm-certificate-expiration-check	Garantisci che l'integrità della rete sia protetta assicurando che i certificati X509 siano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
3.6.1(b)	b) Le BFI devono valutare i requisiti di sicurezza associati ai loro sistemi di internet banking e ad altri sistemi pertinenti e adottare una soluzione di crittografia che tenga conto del grado di riservatezza e integrità richiesto.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(b)	b) Le BFI devono valutare i requisiti di sicurezza associati ai loro sistemi di internet banking e ad altri sistemi pertinenti e adottare una soluzione di crittografia che tenga conto del grado di riservatezza e integrità richiesto.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
3.6.1(b)	b) Le BFI devono valutare i requisiti di sicurezza associati ai loro sistemi di internet banking e ad altri sistemi pertinenti e adottare una soluzione di crittografia che tenga conto del grado di riservatezza e integrità richiesto.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(b)	b) Le BFI devono valutare i requisiti di sicurezza associati ai loro sistemi di internet banking e ad altri sistemi pertinenti e adottare una soluzione di crittografia che tenga conto del grado di riservatezza e integrità richiesto.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.6.1(b)	b) Le BFI devono valutare i requisiti di sicurezza associati ai loro sistemi di internet banking e ad altri sistemi pertinenti e adottare una soluzione di crittografia che tenga conto del grado di riservatezza e integrità richiesto.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(b)	b) Le BFI devono valutare i requisiti di sicurezza associati ai loro sistemi di internet banking e ad altri sistemi pertinenti e adottare una soluzione di crittografia che tenga conto del grado di riservatezza e integrità richiesto.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(b)	b) Le BFI devono valutare i requisiti di sicurezza associati ai loro sistemi di internet banking e ad altri sistemi pertinenti e adottare una soluzione di crittografia che tenga conto del grado di riservatezza e integrità richiesto.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.6.1(b)	b) Le BFI devono valutare i requisiti di sicurezza associati ai loro sistemi di internet banking e ad altri sistemi pertinenti e adottare una soluzione di crittografia che tenga conto del grado di riservatezza e integrità richiesto.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(b)	b) Le BFI devono valutare i requisiti di sicurezza associati ai loro sistemi di internet banking e ad altri sistemi pertinenti e adottare una soluzione di crittografia che tenga conto del grado di riservatezza e integrità richiesto.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
3.6.1(b)	b) Le BFI devono valutare i requisiti di sicurezza associati ai loro sistemi di internet banking e ad altri sistemi pertinenti e adottare una soluzione di crittografia che tenga conto del grado di riservatezza e integrità richiesto.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(d)	d) Le BFI che forniscono servizi di internet banking devono essere reattive nei confronti di condizioni insolite del traffico di rete/prestazioni del sistema e all'improvviso aumento dell'utilizzo delle risorse di sistema, che potrebbe significare un attacco DDoS. Di conseguenza, il successo di qualsiasi azione preventiva e reattiva dipende dall'implementazione di strumenti adeguati per rilevare, monitorare e analizzare efficacemente le anomalie nelle reti e nei sistemi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(d)	d) Le BFI che forniscono servizi di internet banking devono essere reattive nei confronti di condizioni insolite del traffico di rete/prestazioni del sistema e all'improvviso aumento dell'utilizzo delle risorse di sistema, che potrebbe significare un attacco DDoS. Di conseguenza, il successo di qualsiasi azione preventiva e reattiva dipende dall'implementazione di strumenti adeguati per rilevare, monitorare e analizzare efficacemente le anomalie nelle reti e nei sistemi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(d)	d) Le BFI che forniscono servizi di internet banking devono essere reattive nei confronti di condizioni insolite del traffico di rete/prestazioni del sistema e all'improvviso aumento dell'utilizzo delle risorse di sistema, che potrebbe significare un attacco DDoS. Di conseguenza, il successo di qualsiasi azione preventiva e reattiva dipende dall'implementazione di strumenti adeguati per rilevare, monitorare e analizzare efficacemente le anomalie nelle reti e nei sistemi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(d)	d) Le BFI che forniscono servizi di internet banking devono essere reattive nei confronti di condizioni insolite del traffico di rete/prestazioni del sistema e all'improvviso aumento dell'utilizzo delle risorse di sistema, che potrebbe significare un attacco DDoS. Di conseguenza, il successo di qualsiasi azione preventiva e reattiva dipende dall'implementazione di strumenti adeguati per rilevare, monitorare e analizzare efficacemente le anomalie nelle reti e nei sistemi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(d)	d) Le BFI che forniscono servizi di internet banking devono essere reattive nei confronti di condizioni insolite del traffico di rete/prestazioni del sistema e all'improvviso aumento dell'utilizzo delle risorse di sistema, che potrebbe significare un attacco DDoS. Di conseguenza, il successo di qualsiasi azione preventiva e reattiva dipende dall'implementazione di strumenti adeguati per rilevare, monitorare e analizzare efficacemente le anomalie nelle reti e nei sistemi.	api-gw-associated-with-waf	AWS WAF consente di configurare una serie di regole (denominate lista di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1(e)	e) Le BFI devono valutare regolarmente le vulnerabilità in materia di sicurezza delle informazioni e valutare l'efficacia dell'attuale quadro di gestione dei rischi in materia di sicurezza informatica, apportando le modifiche necessarie e per garantire che le vulnerabilità emergenti siano affrontate tempestivamente. Tale valutazione deve essere condotta anche nell'ambito di qualsiasi modifica sostanziale.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.4(a)(b)	a) Limita l'accesso a Internet e separa i sistemi critici dall'ambiente IT generale. b) Riduci la superficie di attacco e le vulnerabilità.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NBC TRMG.

Best practice operative per NERC CIP BCSI

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra gli standard di protezione delle infrastrutture critiche (NERC CIP) della North American Electric Reliability Corporation per BES Cyber System Information (BCSI), CIP-004-7 e CIP-011-3 e le regole gestite. AWS Config Ogni regola AWS Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CIP NERC applicabili a BCSI. Un controllo NERC CIP può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-004-7-R6-Parte 6.1	Ciascuna entità responsabile deve implementare uno o più programmi di gestione degli accessi documentati per autorizzare, verificare e revocare l'accesso fornito a BCSI relativo ai "Sistemi applicabi li" identificati nel CIP-004-7 Tabella R6 – Access Managemen t for BES Cyber System Informati on, che collettiv amente includono ciascuna delle parti dei requisiti applicabi li nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information. Per essere considerato un accesso a BCSI nel contesto di questo requisito, un individuo ha la possibilità di ottenere e di utilizzar e BCSI. L'accesso fornito deve essere considerato il risultato	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini Amazon. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard multi-tenancy e l'autenticazione di base HTTP per e Kibana. OpenSearch OpenSearch

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	delle azioni specifiche intraprese per fornire a uno o più individui i mezzi per accedere a BCSI (ad esempio, può includere chiavi fisiche o carte di accesso, utenti e diritti e privilegi associati , chiavi di crittogra fia). Parte 6.1: Prima dell'assegnazione, autorizza (a meno che non lo sia già ai sensi della Parte 4.1.) in base alle necessità, come stabilito dall'Enti tà Responsabile, ad eccezione delle circostanze ecceziona li del CIP: 6.1.1. Accesso elettronico assegnato al BCSI elettronico		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-004-7-R6-Parte 6.1	Ciascuna entità responsabile deve implementare uno o più programmi di gestione degli accessi documentati per autorizzare, verificare e revocare l'accesso fornito a BCSI relativo ai "Sistemi applicabili" identificati nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information, che collettivamente includono ciascuna delle parti dei requisiti applicabili nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information. Per essere considerato un accesso a BCSI nel contesto di questo requisito, un individuo ha la possibilità di ottenere e di utilizzare BCSI. L'accesso fornito deve essere considerato il risultato	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	delle azioni specifiche intraprese per fornire a uno o più individui i mezzi per accedere a BCSI (ad esempio, può includere chiavi fisiche o carte di accesso, utenti e diritti e privilegi associati , chiavi di crittogra fia). Parte 6.1: Prima dell'assegnazione, autorizza (a meno che non lo sia già ai sensi della Parte 4.1.) in base alle necessità, come stabilito dall'Enti tà Responsabile, ad eccezione delle circostanze ecceziona li del CIP: 6.1.1. Accesso elettronico assegnato al BCSI elettronico		e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-004-7-R6-Parte 6.1	Ciascuna entità responsabile deve implementare uno o più programmi di gestione degli accessi documentati per autorizzare, verificare e revocare l'accesso fornito a BCSI relativo ai "Sistemi applicabili" identificati nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information, che collettivamente includono ciascuna delle parti dei requisiti applicabili nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information. Per essere considerato un accesso a BCSI nel contesto di questo requisito, un individuo ha la possibilità di ottenere e di utilizzare BCSI. L'accesso fornito deve essere considerato il risultato	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	delle azioni specifiche intraprese per fornire a uno o più individui i mezzi per accedere a BCSI (ad esempio, può includere chiavi fisiche o carte di accesso, utenti e diritti e privilegi associati , chiavi di crittogra fia). Parte 6.1: Prima dell'assegnazione, autorizza (a meno che non lo sia già ai sensi della Parte 4.1.) in base alle necessità, come stabilito dall'Enti tà Responsabile, ad eccezione delle circostanze ecceziona li del CIP: 6.1.1. Accesso elettronico assegnato al BCSI elettronico		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-004-7-R6-Parte 6.1	Ciascuna entità responsabile deve implementare uno o più programmi di gestione degli accessi documentati per autorizzare, verificare e revocare l'accesso fornito a BCSI relativo ai "Sistemi applicabili" identificati nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information, che collettivamente includono ciascuna delle parti dei requisiti applicabili nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information. Per essere considerato un accesso a BCSI nel contesto di questo requisito, un individuo ha la possibilità di ottenere e di utilizzare BCSI. L'accesso fornito deve essere considerato il risultato	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	delle azioni specifiche intraprese per fornire a uno o più individui i mezzi per accedere a BCSI (ad esempio, può includere chiavi fisiche o carte di accesso, utenti e diritti e privilegi associati , chiavi di crittogra fia). Parte 6.1: Prima dell'assegnazione, autorizza (a meno che non lo sia già ai sensi della Parte 4.1.) in base alle necessità, come stabilito dall'Enti tà Responsabile, ad eccezione delle circostanze ecceziona li del CIP: 6.1.1. Accesso elettronico assegnato al BCSI elettronico		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-004-7-R6-Parte 6.1	Ciascuna entità responsabile deve implementare uno o più programmi di gestione degli accessi documentati per autorizzare, verificare e revocare l'accesso fornito a BCSI relativo ai "Sistemi applicabili" identificati nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information, che collettivamente includono ciascuna delle parti dei requisiti applicabili nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information. Per essere considerato un accesso a BCSI nel contesto di questo requisito, un individuo ha la possibilità di ottenere e di utilizzare BCSI. L'accesso fornito deve essere considerato il risultato	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	delle azioni specifiche intraprese per fornire a uno o più individui i mezzi per accedere a BCSI (ad esempio, può includere chiavi fisiche o carte di accesso, utenti e diritti e privilegi associati , chiavi di crittogra fia). Parte 6.1: Prima dell'assegnazione, autorizza (a meno che non lo sia già ai sensi della Parte 4.1.) in base alle necessità, come stabilito dall'Enti tà Responsabile, ad eccezione delle circostanze ecceziona li del CIP: 6.1.1. Accesso elettronico assegnato al BCSI elettronico		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-004-7-R6-Parte 6.1	Ciascuna entità responsabile deve implementare uno o più programmi di gestione degli accessi documentati per autorizzare, verificare e revocare l'accesso fornito a BCSI relativo ai "Sistemi applicabili" identificati nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information, che collettivamente includono ciascuna delle parti dei requisiti applicabili nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information. Per essere considerato un accesso a BCSI nel contesto di questo requisito, un individuo ha la possibilità di ottenere e di utilizzare BCSI. L'accesso fornito deve essere considerato il risultato	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	delle azioni specifiche intraprese per fornire a uno o più individui i mezzi per accedere a BCSI (ad esempio, può includere chiavi fisiche o carte di accesso, utenti e diritti e privilegi associati , chiavi di crittogra fia). Parte 6.1: Prima dell'assegnazione, autorizza (a meno che non lo sia già ai sensi della Parte 4.1.) in base alle necessità, come stabilito dall'Enti tà Responsabile, ad eccezione delle circostanze ecceziona li del CIP: 6.1.1. Accesso elettronico assegnato al BCSI elettronico		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-004-7-R6-Parte 6.1	Ciascuna entità responsabile deve implementare uno o più programmi di gestione degli accessi documentati per autorizzare, verificare e revocare l'accesso fornito a BCSI relativo ai "Sistemi applicabili" identificati nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information, che collettivamente includono ciascuna delle parti dei requisiti applicabili nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information. Per essere considerato un accesso a BCSI nel contesto di questo requisito, un individuo ha la possibilità di ottenere e di utilizzare BCSI. L'accesso fornito deve essere considerato il risultato	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	delle azioni specifiche intraprese per fornire a uno o più individui i mezzi per accedere a BCSI (ad esempio, può includere chiavi fisiche o carte di accesso, utenti e diritti e privilegi associati , chiavi di crittogra fia). Parte 6.1: Prima dell'assegnazione, autorizza (a meno che non lo sia già ai sensi della Parte 4.1.) in base alle necessità, come stabilito dall'Enti tà Responsabile, ad eccezione delle circostanze ecceziona li del CIP: 6.1.1. Accesso elettronico assegnato al BCSI elettronico		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-004-7-R6-Parte 6.1	Ciascuna entità responsabile deve implementare uno o più programmi di gestione degli accessi documentati per autorizzare, verificare e revocare l'accesso fornito a BCSI relativo ai "Sistemi applicabili" identificati nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information, che collettivamente includono ciascuna delle parti dei requisiti applicabili nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information. Per essere considerato un accesso a BCSI nel contesto di questo requisito, un individuo ha la possibilità di ottenere e di utilizzare BCSI. L'accesso fornito deve essere considerato il risultato	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	delle azioni specifiche intraprese per fornire a uno o più individui i mezzi per accedere a BCSI (ad esempio, può includere chiavi fisiche o carte di accesso, utenti e diritti e privilegi associati , chiavi di crittogra fia). Parte 6.1: Prima dell'assegnazione, autorizza (a meno che non lo sia già ai sensi della Parte 4.1.) in base alle necessità, come stabilito dall'Enti tà Responsabile, ad eccezione delle circostanze ecceziona li del CIP: 6.1.1. Accesso elettronico assegnato al BCSI elettronico		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-004-7-R6-Parte 6.1	Ciascuna entità responsabile deve implementare uno o più programmi di gestione degli accessi documentati per autorizzare, verificare e revocare l'accesso fornito a BCSI relativo ai "Sistemi applicabili" identificati nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information, che collettivamente includono ciascuna delle parti dei requisiti applicabili nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information. Per essere considerato un accesso a BCSI nel contesto di questo requisito, un individuo ha la possibilità di ottenere e di utilizzare BCSI. L'accesso fornito deve essere considerato il risultato	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	delle azioni specifiche intraprese per fornire a uno o più individui i mezzi per accedere a BCSI (ad esempio, può includere chiavi fisiche o carte di accesso, utenti e diritti e privilegi associati , chiavi di crittogra fia). Parte 6.1: Prima dell'assegnazione, autorizza (a meno che non lo sia già ai sensi della Parte 4.1.) in base alle necessità, come stabilito dall'Enti tà Responsabile, ad eccezione delle circostanze ecceziona li del CIP: 6.1.1. Accesso elettronico assegnato al BCSI elettronico		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-004-7-R6-Parte 6.1	Ciascuna entità responsabile deve implementare uno o più programmi di gestione degli accessi documentati per autorizzare, verificare e revocare l'accesso fornito a BCSI relativo ai "Sistemi applicabili" identificati nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information, che collettivamente includono ciascuna delle parti dei requisiti applicabili nel CIP-004-7 Tabella R6 – Access Management for BES Cyber System Information. Per essere considerato un accesso a BCSI nel contesto di questo requisito, un individuo ha la possibilità di ottenere e di utilizzare BCSI. L'accesso fornito deve essere considerato il risultato	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	delle azioni specifiche intraprese per fornire a uno o più individui i mezzi per accedere a BCSI (ad esempio, può includere chiavi fisiche o carte di accesso, utenti e diritti e privilegi associati , chiavi di crittogra fia). Parte 6.1: Prima dell'assegnazione, autorizza (a meno che non lo sia già ai sensi della Parte 4.1.) in base alle necessità, come stabilito dall'Enti tà Responsabile, ad eccezione delle circostanze ecceziona li del CIP: 6.1.1. Accesso elettronico assegnato al BCSI elettronico		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettivamente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettivamente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettivamente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettivamente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettivamente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configura ti per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilita zione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettivamente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	ecr-private-tag-immutability-enabled	Abilita l'immutabilità dei tag di Elastic Container Repository (ECR) per evitare che i tag di immagine sulle immagini ECR vengano sovrascritti. In precedenza, i tag potevano essere sovrascritti, richiedendo metodologie manuali per identificare in modo univoco un'immagine.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	ecs-containers-rea donly-access	L'abilitazione dell'acce sso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettar e il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificat o a meno che non disponga di autorizza zioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	kms-cmk-not-schedu led-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianifica ta l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (KMS).AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificar e tutte le chiavi per le quali è pianifica ta l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzion ale.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettivamente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearc h Service all'inter no di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearc h di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservaz ione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibi lità.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettivamente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettivamente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizz o di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	s3-event-notifications-enabled	Le notifiche degli eventi di Amazon S3 possono notificar e al personale competente eventuali modifiche accidenta li o intenzionali agli oggetti del bucket. Gli avvisi includono: creazione di un nuovo oggetto, rimozione di oggetti, ripristino di oggetti, oggetti persi e replicati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	s3-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazion i che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	sagemaker-endpoint -configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	rds-cluster-default-admin-check	Poiché i nomi utente predefiniti sono di dominio pubblico, la loro modifica può aiutare a ridurre la superficie di attacco dei cluster database Amazon Relationa l Database Service (Amazon RDS).

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	rds-instance-default-admin-check	Poiché i nomi utente predefiniti sono di dominio pubblico, la loro modifica può aiutare a ridurre la superficie di attacco per le istanze database Amazon Relational Database Service (Amazon RDS).

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	redshift-default-admin-check	Poiché i nomi utente predefiniti sono di dominio pubblico, la loro modifica può aiutare a ridurre la superficie di attacco dei cluster Amazon Redshift.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CIP-011-3-R1-Parte 1.2	Ciascuna entità responsabile deve implementare uno o più programmi documentati di protezione delle informazioni che includono collettiv amente ciascuna delle parti dei requisiti applicabili nel CIP-011-3 Tabella R1 – Protezione delle informazioni. Parte 1.2: Metodi per proteggere e gestire in modo sicuro il BCSI per mitigare i rischi di compromissione della riservatezza.	s3-bucket-acl-proh ibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi sui bucket Amazon S3. Gli ACL sono meccanism i di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzar e le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NERC CIP BCSI.

Best practice operative per i principi di sicurezza cloud NCSC

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra i principi di sicurezza del cloud del National Cyber Security Centre (NCSC) del Regno Unito e le regole di Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli dei Principi di sicurezza del cloud NCSC del Regno Unito. Un controllo dei principi di sicurezza cloud NCSC del Regno Unito può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo modello di pacchetto di conformità di esempio contiene mappature ai controlli secondo i principi di sicurezza del cloud NCSC del Regno Unito (National Cyber Security Centre | Cloud security guidance), con tali informazioni del settore pubblico concesse in licenza ai sensi della Open Government Licence v3.0. È possibile accedere alla Open Government Licence qui: Open Government License for Public Sector Information.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1. Protezione dei dati in transito	Le reti di transito dei dati degli utenti devono essere adeguatamente protette da manomissioni e eavesdropping.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
1. Protezione dei dati in transito	Le reti di transito dei dati degli utenti devono essere adeguatamente	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	protette da manomissioni e eavesdropping.		ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
1. Protezione dei dati in transito	Le reti di transito dei dati degli utenti devono essere adeguatamente protette da manomissioni e eavesdropping.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1. Protezione dei dati in transito	Le reti di transito dei dati degli utenti devono essere adeguatamente protette da manomissioni e eavesdropping.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
1. Protezione dei dati in transito	Le reti di transito dei dati degli utenti devono essere adeguatamente protette da manomissioni e eavesdropping.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1. Protezione dei dati in transito	Le reti di transito dei dati degli utenti devono essere adeguatamente protette da manomissioni e eavesdropping.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
1. Protezione dei dati in transito	Le reti di transito dei dati degli utenti devono essere adeguatamente protette da manomissioni e eavesdropping.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1. Protezione dei dati in transito	Le reti di transito dei dati degli utenti devono essere adeguatamente protette da manomissioni e eavesdropping.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
1. Protezione dei dati in transito	Le reti di transito dei dati degli utenti devono essere adeguatamente protette da manomissioni e eavesdropping.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1. Protezione dei dati in transito	Le reti di transito dei dati degli utenti devono essere adeguatamente protette da manomissioni e eavesdropping.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
1. Protezione dei dati in transito	Le reti di transito dei dati degli utenti devono essere adeguatamente protette da manomissioni e eavesdropping.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	account-part-of-or ganizations	La gestione centraliz zata Account AWS all'interno di AWS Organizations aiuta a garantire la conformit à degli account. L'assenza di una governance centraliz zata degli account può comportar e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatamente protetti.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	elb-deletion-prote ction-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciam ento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	kinesis-stream-enc rypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatamente protetti.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	s3-account-level-p ublic-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltati vamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPubl icPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPubl icAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatamente protetti.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazi one predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	kms-cmk-not-schedu led-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianifica ta l'eliminazione delle chiavi master del cliente (CMK) necessarie in AWS Key Managemen t Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificar e tutte le chiavi per le quali è pianifica ta l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzion ale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatamente protetti.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatamente protetti.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatamente protetti.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatamente protetti.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	s3-bucket-level-pu blic-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	sagemaker-endpoint -configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	sagemaker-notebook -instance-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatamente protetti.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2. Protezione e resilienza degli asset	I tuoi dati (e le risorse che li archiviano o li elaborano) devono essere adeguatam ente protetti.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	account-part-of-or ganizations	La gestione centraliz zata Account AWS all'interno di AWS Organizations aiuta a garantire la conformit à degli account. L'assenza di una governance centraliz zata degli account può comportar e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorar e la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
5. Sicurezza operativa	I servizi devono essere utilizzati ù e gestiti in modo da impedire, rilevare o prevenire gli attacchi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7. Sviluppo sicuro	I servizi cloud devono essere progettati, sviluppati e implementati in modo da ridurre al minimo e mitigare le minacce alla loro sicurezza.	codebuild-project-environment-privileged-check	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che il tuo ambiente di CodeBuild progetto Amazon non abbia la modalità privilegiata abilitata. Questa impostazione deve essere disabilitata per impedire l'accesso involontario alle API Docker e all'hardware sottostante del container.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7. Sviluppo sicuro	I servizi cloud devono essere progettati, sviluppati e implementati in modo da ridurre al minimo e mitigare le minacce alla loro sicurezza.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7. Sviluppo sicuro	I servizi cloud devono essere progettati, sviluppati e implementati in modo da ridurre al minimo e mitigare le minacce alla loro sicurezza.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9. Gestione utenti sicura	I fornitori devono mettere a disposizione gli strumenti per gestire in modo sicuro l'utilizzo del loro servizio.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9. Gestione utenti sicura	I fornitori devono mettere a disposizione gli strumenti per gestire in modo sicuro l'utilizzo del loro servizio.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9. Gestione utenti sicura	I fornitori devono mettere a disposizione gli strumenti per gestire in modo sicuro l'utilizzo del loro servizio.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
9. Gestione utenti sicura	I fornitori devono mettere a disposizione gli strumenti per gestire in modo sicuro l'utilizzo del loro servizio.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9. Gestione utenti sicura	I fornitori devono mettere a disposizione gli strumenti per gestire in modo sicuro l'utilizzo del loro servizio.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9. Gestione utenti sicura	I fornitori devono mettere a disposizione gli strumenti per gestire in modo sicuro l'utilizzo del loro servizio.	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9. Gestione utenti sicura	I fornitori devono mettere a disposizione gli strumenti per gestire in modo sicuro l'utilizzo del loro servizio.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9. Gestione utenti sicura	I fornitori devono mettere a disposizione gli strumenti per gestire in modo sicuro l'utilizzo del loro servizio.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9. Gestione utenti sicura	I fornitori devono mettere a disposizione gli strumenti per gestire in modo sicuro l'utilizzo del loro servizio.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9. Gestione utenti sicura	I fornitori devono mettere a disposizione gli strumenti per gestire in modo sicuro l'utilizzo del loro servizio.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
9. Gestione utenti sicura	I fornitori devono mettere a disposizione gli strumenti per gestire in modo sicuro l'utilizzo del loro servizio.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
9. Gestione utenti sicura	I fornitori devono mettere a disposizione gli strumenti per gestire in modo sicuro l'utilizzo del loro servizio.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10. Identità e autenticazione	L'accesso alle interfacce di servizio deve essere limitato a persone autenticate e autorizzate.	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10. Identità e autenticazione	L'accesso alle interfacce di servizio deve essere limitato a persone autenticate e autorizzate.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10. Identità e autenticazione	L'accesso alle interfacce di servizio deve essere limitato a persone autenticate e autorizzate.	rds-instance-iam-authentication-enabled	Assicurati che l'autenticazione AWS Identity and Access Management (IAM) sia abilitata sulle istanze di Amazon Relational Database Service (Amazon RDS) per controllare l'accesso a sistemi e asset. In questo modo il traffico di rete da e verso il database viene crittografato utilizzando Secure Sockets Layer (SSL). Non devi archiviare le credenziali dell'utente nel database, perché l'autenticazione è gestita esternamente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10. Identità e autenticazione	L'accesso alle interfacce di servizio deve essere limitato a persone autenticate e autorizzate.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
10. Identità e autenticazione	L'accesso alle interfacce di servizio deve essere limitato a persone autenticate e autorizzate.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10. Identità e autenticazione	L'accesso alle interfacce di servizio deve essere limitato a persone autenticate e autorizzate.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10. Identità e autenticazione	L'accesso alle interfacce di servizio deve essere limitato a persone autenticate e autorizzate.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10. Identità e autenticazione	L'accesso alle interfacce di servizio deve essere limitato a persone autenticate e autorizzate.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10. Identità e autenticazione	L'accesso alle interfacce di servizio deve essere limitato a persone autenticate e autorizzate.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10. Identità e autenticazione	L'accesso alle interfacce di servizio deve essere limitato a persone autenticate e autorizzate.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicuran do che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	ecs-container-insights-enabled	Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon Elastic Container Service (ECS) e delle tue AWS soluzioni. Container Insights fornisce inoltre informazioni diagnostiche, ad esempio errori di riavvio del container, che consentono di isolare i problemi e risolverli in modo rapido.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	ecs-containers-non privileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizio ni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettar e il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificat o a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicuran do che i nodi master del cluster Amazon EMR non siano accessibili pubblicam ente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearc h Service all'inter no di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11. Protezione da interfaccia esterna	Tutte le interfacc e esterne o meno affidabili al servizio devono essere identificate e difese.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
12. Amministrazione dei servizi sicura	I fornitori di servizi cloud devono riconoscere l'elevato valore dei sistemi di amministrazione.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
13. Audit delle informazioni per gli utenti	I fornitori devono fornire i log necessari per monitorare l'accesso al servizio e i dati in esso contenuti .	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
13. Audit delle informazioni per gli utenti	I fornitori devono fornire i log necessari per monitorare l'accesso al servizio e i dati in esso contenuti .	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
13. Audit delle informazioni per gli utenti	I fornitori devono fornire i log necessari per monitorare l'accesso al servizio e i dati in esso contenuti .	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail log. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
13. Audit delle informazioni per gli utenti	I fornitori devono fornire i log necessari per monitorare l'accesso al servizio e i dati in esso contenuti .	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NCSC Cloud Security Principles.

Best practice operative per NCSC Cyber Assessment Framework

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra i controlli del Cyber Assessment Framework (CAF) del National Cyber Security Centre (NCSC) del Regno Unito e le regole Config gestite. AWS Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli CAF NCSC del Regno Unito. Un controllo CAF NCSC del Regno Unito può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo modello di pacchetto di conformità di esempio contiene mappature ai controlli all'interno del NCSC CAF (National Cyber Security Centre | NCSC CAF guidance) del Regno Unito, con tali

informazioni del settore pubblico concesse in licenza ai sensi della Open Government Licence v3.0. È possibile accedere alla Open Government Licence qui: Open Government License for Public Sector Information.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
A3.a Gestione degli asset	Tutte le informazioni finalizzate a fornire, mantenere o supportare reti e sistemi informativi necessari per l'operatività delle funzioni essenziali sono determinate e comprese. Il complesso delle informazioni include dati, persone e sistemi, nonché qualsiasi infrastruttura di supporto (come alimentazione o raffreddamento).	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.
A3.a Gestione degli asset	Tutte le informazioni finalizzate a fornire, mantenere o supportare reti e sistemi informativi necessari per l'operatività delle funzioni essenziali sono determinate e comprese. Il complesso delle	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	informazioni include dati, persone e sistemi, nonché qualsiasi infrastru ttura di supporto (come alimentazione o raffreddamento).		Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.
A3.a Gestione degli asset	Tutte le informazi oni finalizzate a fornire, mantenere o supportare reti e sistemi informati vi necessari per l'operatività delle funzioni essenzial i sono determina te e comprese. Il complesso delle informazioni include dati, persone e sistemi, nonché qualsiasi infrastru ttura di supporto (come alimentazione o raffreddamento).	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
A3.a Gestione degli asset	Tutte le informazioni finalizzate a fornire, mantenere o supportare reti e sistemi informativi necessari per l'operatività delle funzioni essenziali sono determinate e comprese. Il complesso delle informazioni include dati, persone e sistemi, nonché qualsiasi infrastruttura di supporto (come alimentazione o raffreddamento).	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
A3.a Gestione degli asset	Tutte le informazioni finalizzate a fornire, mantenere o supportare reti e sistemi informativi necessari per l'operatività delle funzioni essenziali sono determinate e comprese. Il complesso delle informazioni include dati, persone e sistemi, nonché qualsiasi infrastruttura di supporto (come alimentazione o raffreddamento).	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autentica zione e Autorizza zione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenzial e.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autenticazione e Autorizzazione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenziale.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autentica zione e Autorizza zione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenzial e.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autenticazione e Autorizzazione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenziale.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autenticazione e Autorizzazione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenziale.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autenticazione e Autorizzazione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenziale.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autentica zione e Autorizza zione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenzial e.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autentica zione e Autorizza zione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenzial e.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autenticazione e Autorizzazione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenziale.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autenticazione e Autorizzazione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenziale.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autentica zione e Autorizza zione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenzial e.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autentica zione e Autorizza zione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenzial e.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autentica zione e Autorizza zione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenzial e.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearc h

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.a Verifica di Identità, Autentica zione e Autorizza zione	Verifica, autentica e autorizza in modo affidabile l'accesso alle reti e ai sistemi informativi che supportano la tua funzionalità essenzial e.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
B2.b Gestione dei dispositivi	Conosci i dispositivi utilizzati per accedere a reti, sistemi informativi e dati che supportano le funzioni essenziali e li utilizzi con fiducia.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.b Gestione dei dispositivi	Conosci i dispositivi utilizzati per accedere a reti, sistemi informativi e dati che supportano le funzioni essenziali e li utilizzi con fiducia.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	codebuild-project-environment-privileged-check	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che il tuo ambiente di CodeBuild progetto Amazon non abbia la modalità privilegiata abilitata. Questa impostazione deve essere disabilitata per impedire l'accesso involontario alle API Docker e all'hardware sottostante del container.
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	ecs-containers-nonprivileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	secretsmanager-secret-unused	Se in AWS Secrets Manager sono presenti credenziali inutilizzate, è necessario disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola consente di impostare un valore su unusedForDays (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazi one che supportano la funzionalità essenzial e.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.c Gestione degli utenti con privilegi	Gestisci in modo rigoroso l'accesso degli utenti con privilegi alle reti e ai sistemi di informazione che supportano la funzionalità essenziale.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d#Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B2.d Identity and Access Management (IdAM)	Garantisci una buona gestione e manutenzione del controllo di identità e accessi per le reti e i sistemi di informazione che supportano la funzionalità essenziale.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.a Comprensione dei dati	Hai una buona conoscenza dei dati importanti per il funzionamento della funzionalità essenziale, dove sono archiviati, dove vengono trasferiti e in che modo l'indisponibilità o l'accesso, la modifica o l'eliminazione non autorizzati possono avere un impatto negativo sulla funzionalità essenziale. Ciò vale anche per terze parti che archiviano dati importanti o vi accedono ai fini del funzionamento della funzionalità essenziale.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	acm-certificate-ex piration-check	Garantisci la protezion e dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExp iration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configura ti per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	s3-bucket-ssl-requ ests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizz o di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	ec2-instance-no-pu blic-ip	Gestisci l'accesso al AWS cloud assicuran do che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicuran do che i nodi master del cluster Amazon EMR non siano accessibili pubblicam ente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	internet-gateway-a uthorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consenton o l'accesso bidirezio nale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtraggio basato sullo stato del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	elb-deletion-prote ction-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciam ento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	opensearch-node-to -node-encryption-c heck	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.b Dati in transito	Hai protetto il transito di dati important i per il funzionam ento della funzional ità essenziale. Ciò include il trasferim ento di dati a terzi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearc h Service all'inter no di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazi one predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	rds-snapshot-encry pted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	sagemaker-notebook -instance-kms-key- configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	kms-cmk-not-schedu led-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianifica ta l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Managemen t Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificar e tutte le chiavi per le quali è pianifica ta l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzion ale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	dynamodb-pitr-enab led	Abilita questa regola per verificare che sia stato eseguito il backup delle informazi oni. Inoltre, mantiene i backup assicuran do che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristin o mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	ebs-optimized-inst ance	Un'istanza ottimizza ta in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/ O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B3.c Dati archiviati	Hai protetto i dati archiviati important i per mantenere operativa la funzional ità essenziale.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
B3.c Dati archiviati	Hai protetto i dati archiviati importanti per mantenere operativa la funzionalità essenziale.	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
B3.c Dati archiviati	Hai protetto i dati archiviati importanti per mantenere operativa la funzionalità essenziale.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtraggio basato sullo stato del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operati vità della funzione essenziale non venga compromes sa dallo sfruttamento di nessuna singola vulnerabilità.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.a Sicuro fin dalla progettazione	Progetti la sicurezza nella rete e nei sistemi informativi che supportano il funzionamento delle funzioni essenziali. Riduci al minimo la superficie di attacco e assicurati che l'operatività della funzione essenziale non venga compromessa dallo sfruttamento di nessuna singola vulnerabilità.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.b Configurazione sicura	Configura in modo sicuro la rete e i sistemi informativi che supportano il funzionamento delle funzioni essenziali.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.b Configurazione sicura	Configura in modo sicuro la rete e i sistemi informativi che supportano il funzionamento delle funzioni essenziali.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.b Configurazione sicura	Configura in modo sicuro la rete e i sistemi informativi che supportano il funzionamento delle funzioni essenziali.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.b Configurazione sicura	Configura in modo sicuro la rete e i sistemi informativi che supportano il funzionamento delle funzioni essenziali.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.c Gestione sicura	Gestisci la rete e i sistemi informativi della tua organizza zione che supportan o l'operatività delle funzioni essenziali per abilitare e mantenere la sicurezza.	ec2-managedinstanc e-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.c Gestione sicura	Gestisci la rete e i sistemi informativi della tua organizza zione che supportan o l'operatività delle funzioni essenziali per abilitare e mantenere la sicurezza.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.c Gestione sicura	Gestisci la rete e i sistemi informativi della tua organizzazione che supportano l'operatività delle funzioni essenziali per abilitare e mantenere la sicurezza.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.d. Vulnerability Management	Gestisci le vulnerabilità note nella rete e nei sistemi informativi per prevenire impatti negativi sulle funzionalità essenziali.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.d. Vulnerability Management	Gestisci le vulnerabilità note nella rete e nei sistemi informativi per prevenire impatti negativi sulle funzionalità essenziali.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.d. Vulnerability Management	Gestisci le vulnerabilità note nella rete e nei sistemi informativi per prevenire impatti negativi sulle funzionalità essenziali.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.d. Vulnerability Management	Gestisci le vulnerabilità note nella rete e nei sistemi informativi per prevenire impatti negativi sulle funzionalità essenziali.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.d. Vulnerability Management	Gestisci le vulnerabilità note nella rete e nei sistemi informativi per prevenire impatti negativi sulle funzionalità essenziali.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B4.d. Vulnerability Management	Gestisci le vulnerabilità note nella rete e nei sistemi informativi per prevenire impatti negativi sulle funzionalità essenziali.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B5.b Progettazione per la resilienza	Progetta la rete e i sistemi informativi che supportano le funzionalità essenziali in modo che siano resilienti agli incidenti di sicurezza informatica. I sistemi sono adeguatamente separati e le limitazioni delle risorse sono mitigate.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B5.b Progettazione per la resilienza	Progetta la rete e i sistemi informativi che supportano le funzionalità essenzial i in modo che siano resilienti agli incidenti di sicurezza informati ca. I sistemi sono adeguatamente separati e le limitazio ni delle risorse sono mitigate.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
B5.b Progettazione per la resilienza	Progetta la rete e i sistemi informativi che supportano le funzionalità essenziali in modo che siano resilienti agli incidenti di sicurezza informatica. I sistemi sono adeguatamente separati e le limitazioni delle risorse sono mitigate.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B5.c Backup	Disponi di backup aggiornati accessibili e protetti dei dati e delle informazioni necessarie per ripristinare l'operatività delle funzioni essenziali	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B5.c Backup	Disponi di backup aggiornati accessibili e protetti dei dati e delle informazioni necessarie per ripristinare l'operatività delle funzioni essenziali	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B5.c Backup	Disponi di backup aggiornati accessibili e protetti dei dati e delle informazioni necessarie per ripristinare l'operatività delle funzioni essenziali	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B5.c Backup	Disponi di backup aggiornati accessibili e protetti dei dati e delle informazioni necessarie per ripristinare l'operatività delle funzioni essenziali	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B5.c Backup	Disponi di backup aggiornati accessibili e protetti dei dati e delle informazioni necessarie per ripristinare l'operatività delle funzioni essenziali	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B5.c Backup	Disponi di backup aggiornati accessibili e protetti dei dati e delle informazioni necessarie per ripristinare l'operatività delle funzioni essenziali	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B5.c Backup	Disponi di backup aggiornati accessibili e protetti dei dati e delle informazioni necessarie per ripristinare l'operatività delle funzioni essenziali	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B5.c Backup	Disponi di backup aggiornati accessibili e protetti dei dati e delle informazioni necessarie per ripristinare l'operatività delle funzioni essenziali	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B5.c Backup	Disponi di backup aggiornati accessibili e protetti dei dati e delle informazioni necessarie per ripristinare l'operatività delle funzioni essenziali	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
B5.c Backup	Disponi di backup aggiornati accessibili e protetti dei dati e delle informazioni necessarie per ripristinare l'operatività delle funzioni essenziali	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.a Copertura del monitoraggio	Le origini dati incluse nel monitoraggio consentono l'identif icazione tempestiv a degli eventi di sicurezza che potrebbero influire sull'operatività delle funzioni essenziali.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.a Copertura del monitoraggio	Le origini dati incluse nel monitoraggio consentono l'identif icazione tempestiv a degli eventi di sicurezza che potrebbero influire sull'operatività delle funzioni essenziali.	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.a Copertura del monitoraggio	Le origini dati incluse nel monitoraggio consentono l'identif icazione tempestiv a degli eventi di sicurezza che potrebbero influire sull'operatività delle funzioni essenziali.	dynamodb-throughpu t-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissi one assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportar e. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficien ti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissi one effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltati vamente i parametri AccountRCU ThresholdPercentag e (Config Default: 80) e AccountWCU ThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
C1.a Copertura del monitoraggio	Le origini dati incluse nel monitoraggio consentono l'identif icazione tempestiv a degli eventi di sicurezza che potrebbero influire sull'operatività delle funzioni essenziali.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitorag gio relativi all'istanza a intervalli di 1 minuto.
C1.a Copertura del monitoraggio	Le origini dati incluse nel monitoraggio consentono l'identif icazione tempestiv a degli eventi di sicurezza che potrebbero influire sull'operatività delle funzioni essenziali.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.a Copertura del monitoraggio	Le origini dati incluse nel monitoraggio consentono l'identificazione tempestiva degli eventi di sicurezza che potrebbero influire sull'operatività delle funzioni essenziali.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.a Copertura del monitoraggio	Le origini dati incluse nel monitoraggio consentono l'identif icazione tempestiv a degli eventi di sicurezza che potrebbero influire sull'operatività delle funzioni essenziali.	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.
C1.a Copertura del monitoraggio	Le origini dati incluse nel monitoraggio consentono l'identif icazione tempestiv a degli eventi di sicurezza che potrebbero influire sull'operatività delle funzioni essenziali.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.a Copertura del monitoraggio	Le origini dati incluse nel monitoraggio consentono l'identificazione tempestiva degli eventi di sicurezza che potrebbero influire sull'operatività delle funzioni essenziali.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.a Copertura del monitoraggio	Le origini dati incluse nel monitoraggio consentono l'identif icazione tempestiv a degli eventi di sicurezza che potrebbero influire sull'operatività delle funzioni essenziali.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.a Copertura del monitoraggio	Le origini dati incluse nel monitoraggio consentono l'identif icazione tempestiv a degli eventi di sicurezza che potrebbero influire sull'operatività delle funzioni essenziali.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.b Proteggere i log	Conserva i dati di log in modo sicuro e concedi l'accesso in lettura solo agli account con esigenze aziendali. Nessun dipendente dovrebbe mai aver bisogno di modificare o eliminare i dati di log entro un periodo di conservazione concordato, dopodiché devono essere eliminati.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.b Proteggere i log	Conserva i dati di log in modo sicuro e concedi l'accesso in lettura solo agli account con esigenze aziendali. Nessun dipendente dovrebbe mai aver bisogno di modificare o eliminare i dati di log entro un periodo di conservazione concordato, dopodiché devono essere eliminati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
C1.b Proteggere i log	Conserva i dati di log in modo sicuro e concedi l'accesso in lettura solo agli account con esigenze aziendali. Nessun dipendente dovrebbe mai aver bisogno di modificare o eliminare i dati di log entro un periodo di conservazione concordato, dopodiché devono essere eliminati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.b Proteggere i log	Conserva i dati di log in modo sicuro e concedi l'accesso in lettura solo agli account con esigenze aziendali. Nessun dipendente dovrebbe mai aver bisogno di modificare o eliminare i dati di log entro un periodo di conservazione concordato, dopodiché devono essere eliminati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
C1.b Proteggere i log	Conserva i dati di log in modo sicuro e concedi l'accesso in lettura solo agli account con esigenze aziendali. Nessun dipendente dovrebbe mai aver bisogno di modificare o eliminare i dati di log entro un periodo di conservazione concordato, dopodiché devono essere eliminati.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.b Proteggere i log	Conserva i dati di log in modo sicuro e concedi l'accesso in lettura solo agli account con esigenze aziendali. Nessun dipendente dovrebbe mai aver bisogno di modificare o eliminare i dati di log entro un periodo di conservazione concordato, dopodiché devono essere eliminati.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.b Proteggere i log	Conserva i dati di log in modo sicuro e concedi l'accesso in lettura solo agli account con esigenze aziendali. Nessun dipendente dovrebbe mai aver bisogno di modificare o eliminare i dati di log entro un periodo di conservazione concordato, dopodiché devono essere eliminati.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.b Proteggere i log	Conserva i dati di log in modo sicuro e concedi l'accesso in lettura solo agli account con esigenze aziendali. Nessun dipendente dovrebbe mai aver bisogno di modificare o eliminare i dati di log entro un periodo di conservazione concordato, dopodiché devono essere eliminati.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
C1.b Proteggere i log	Conserva i dati di log in modo sicuro e concedi l'accesso in lettura solo agli account con esigenze aziendali. Nessun dipendente dovrebbe mai aver bisogno di modificare o eliminare i dati di log entro un periodo di conservazione concordato, dopodiché devono essere eliminati.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.b Proteggere i log	Conserva i dati di log in modo sicuro e concedi l'accesso in lettura solo agli account con esigenze aziendali. Nessun dipendente dovrebbe mai aver bisogno di modificare o eliminare i dati di log entro un periodo di conservazione concordato, dopodiché devono essere eliminati.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.b Proteggere i log	Conserva i dati di log in modo sicuro e concedi l'accesso in lettura solo agli account con esigenze aziendali. Nessun dipendente dovrebbe mai aver bisogno di modificare o eliminare i dati di log entro un periodo di conservazione concordato, dopodiché devono essere eliminati.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenziali incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenzial i incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenzial i incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	s3-event-notifications-enabled	Le notifiche degli eventi di Amazon S3 possono notificar e al personale competente eventuali modifiche accidenta li o intenzionali agli oggetti del bucket. Gli avvisi includono: creazione di un nuovo oggetto, rimozione di oggetti, ripristino di oggetti, oggetti persi e replicati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenzial i incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenziali incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
C1.c Generazione di avvisi	Le prove di potenziali incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenzial i incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
C1.c Generazione di avvisi	Le prove di potenzial i incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenziali incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenzial i incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicaz ione centrale all'inter no di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettaglia te sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenzial i incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenzial i incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenziali incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenzial i incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenziali incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.c Generazione di avvisi	Le prove di potenzial i incidenti di sicurezza contenute nei dati di monitoraggio vengono identificate in modo affidabile e attivano gli avvisi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.d Identificazione degli incidenti di sicurezza	Contestualizza gli avvisi conoscendo la minaccia e i sistemi in uso, per identificare gli incidenti di sicurezza che richiedono una qualche forma di risposta.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.d Identificazione degli incidenti di sicurezza	Contestualizza gli avvisi conoscendo la minaccia e i sistemi in uso, per identificare gli incidenti di sicurezza che richiedono una qualche forma di risposta.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.e Strumenti e competenze di monitoraggio	Il monitoraggio delle competenze, degli strumenti e dei ruoli del personale, compresi quelli in outsourcing, deve riflettere i requisiti di governance e segnalazione, le minacce previste e la complessità della rete o dei dati di sistema che devono utilizzare. Il personale addetto al monitoraggio conosce le funzioni essenziali che deve proteggere.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.e Strumenti e competenze di monitoraggio	Il monitoraggio delle competenze, degli strumenti e dei ruoli del personale , compresi quelli in outsourcing, deve riflettere i requisiti di governance e segnalazione, le minacce previste e la complessità della rete o dei dati di sistema che devono utilizzare. Il personale addetto al monitoraggio conosce le funzioni essenziali che deve proteggere.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C1.e Strumenti e competenze di monitoraggio	Il monitoraggio delle competenze, degli strumenti e dei ruoli del personale , compresi quelli in outsourcing, deve riflettere i requisiti di governance e segnalazione, le minacce previste e la complessità della rete o dei dati di sistema che devono utilizzare. Il personale addetto al monitoraggio conosce le funzioni essenziali che deve proteggere.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C2.a Anomalie del sistema per il rilevamento degli attacchi	Definisci esempi di anomalie nel comportamento del sistema che forniscono metodi pratici per rilevare attività dannose altrimenti difficili da identificare.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
C2.a Anomalie del sistema per il rilevamento degli attacchi	Definisci esempi di anomalie nel comportamento del sistema che forniscono metodi pratici per rilevare attività dannose altrimenti difficili da identificare.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
D1.c Test ed esercizi	L'organizzazione esegue esercizi per testare i piani di risposta, utilizzando gli incidenti passati che hanno interessato la tua organizzazione (e anche altre) e scenari che si basano sull'intelligence delle minacce e sulla valutazione del rischio.	response-plan-exists-maintained (Controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti. Disporre di piani di risposta aggiornati e formalmente documentati può aiutare a garantire che il personale addetto all'intervento comprenda ruoli, responsabilità e processi da seguire durante un incidente.
D1.c Test ed esercizi	L'organizzazione esegue esercizi per testare i piani di risposta, utilizzando gli incidenti passati che hanno interessato la tua organizzazione (e anche altre) e scenari che si basano sull'intelligence delle minacce e sulla valutazione del rischio.	response-plan-tested (Controllo del processo)	Verifica che i piani di risposta agli incidenti e di ripristino siano testati. Questo può aiutare a capire se il piano sarà efficace in caso di incidente e se è necessario risolvere eventuali lacune o apportare aggiornamenti.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NCSC Cyber Assessment Framework.

Best practice operative per servizi di rete e distribuzione di contenuti

Questo pacchetto di conformità contiene AWS Config regole basate sui servizi di rete e distribuzione dei contenuti. Per ulteriori informazioni, vedere Networking and Content Delivery su. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best practice for Networking and Content Delivery Services.

Best practice operative per NIST 800-53 rev 4

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il NIST 800-53 e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli NIST 800-53. Un controllo NIST 800-53 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo Conformance Pack è stato convalidato da AWS Security Assurance Services LLC (AWS SAS), che è un team di Payment Card Industry Qualified Security Assessors (QSA), HITRUST Certified Common Security Framework Practitioners (ccSFP) e professionisti della conformità certificati per fornire linee guida e valutazioni per vari framework di settore. AWS I professionisti SAS hanno progettato questo Conformance Pack per consentire a un cliente di allinearsi a un sottoinsieme del NIST 800-53.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(1)	L'organizzazione utilizza meccanismi automatizzati per supportare la gestione degli account dei sistemi informativi.	secretsmanager-scheduled-rotation-success-controlla	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.
AC-2(1)	L'organizzazione utilizza meccanismi automatizzati per supportare la gestione degli account dei sistemi informativi.	iam-user-group-membership-controlla	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti indicati dal NIST SP 800-63 e dal benchmark Centers for Internet Security (CIS) AWS Foundations per quanto riguarda la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foun dational Security Best Practices value: true), RequireSy mbols (AWS Foun dational Security Best Practices value: true), RequireNu

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			mbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizza tiva. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	iam-user-unused-cr edentials-controlla	AWS Identity and Access Managemen t (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controlla ndo le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizz ate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegi o minimo. Questa regola richiede di impostare un valore su maxCreden tialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(1)	L'organizzazione utilizza meccanism i automatizzati per supportare la gestione degli account dei sistemi informativi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(3)	Il sistema informativo disattiva automaticamente gli account inattivi dopo [Assegnazione: periodo di tempo definito dall'organizzazione].	iam-user-unused-credentials-controlla	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(4)	Il sistema informati vo verifica automatic amente le operazioni di creazione, modifica, abilitazione, disabilit azione e rimozione degli account e notifica [Assegnaz ione: personale o ruoli definiti dall'orga nizzazione].	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	cloud-trail-cloud-watch-abilitati ai log	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail invierà i file di registro da tutti Regioni AWS al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS lancia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(4)	Il sistema informativo verifica automaticamente le operazioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account e notifica [Assegnazione: personale o ruoli definiti dall'organizzazione].	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(12)(a)	L'organizzazione: a. Monitora gli account del sistema informati vo per [Assegnazione: uso atipico definito dall'organizzazione].	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(12)(a)	L'organizzazione: a. Monitora gli account del sistema informativo per [Assegnazione: uso atipico definito dall'organizzazione].	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-user-unused-credentials-controlla	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dal benchmark Centers for Internet Security (CIS) AWS Foundations per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foun

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			dational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(f)	L'organizzazione: f. Crea, abilita, modifica, disabilita e rimuove gli account del sistema informativo in conformità a [Assegnazione: procedure o condizioni definite dall'organizzazione].	iam-root-access-key-controlla	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	s3- bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli Account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(g)	L'organizzazione: g. Monitora l'uso degli account del sistema informativo.	cloud-trail-cloud-watch-abilitati ai log	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AC-2(j)	L'organizzazione: j. Verifica la conformit à degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	root-account-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	secretsmanager-scheduled-rotation-success-controlla	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-user-group-membership-controlla	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dal benchmark Centers for Internet Security (CIS) AWS Foundations per quanto riguarda la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNu

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			mbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-root-access-key-controlla	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformit à degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			e altre informazioni amministrative su ogni principale.
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-group-has-users-controlla	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformità degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-2(j)	L'organizzazione: j. Verifica la conformit à degli account ai requisiti di gestione degli account [Assegnazione: frequenza definita dall'organizzazione].	iam-user-no-policies-controlla	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
AC-3	Il sistema informativo applica le autorizza zioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	s3- bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-user-no-policies-controlla	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-user-unused-credentials-controlla	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	lambda-function-public-access-proibito	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-3	Il sistema informativo applica le autorizza zioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	redshift-cluster-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
AC-3	Il sistema informativo applica le autorizza zioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	s-3 bucket-policy-gran tee-check	Gestisci l'accesso al AWS cloud abilitand o s3_ bucket_po licy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-user-group-membership-controlla	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	s3- bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	blocchi s3 account-level-public-access	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-root-access-key-controlla	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	ebs-snapshot-public-restorable-controlla	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-3	Il sistema informativo applica le autorizza zioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			e altre informazioni amministrative su ogni principale.
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-group-has-users-controlla	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-3	Il sistema informativo applica le autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.	sagemaker-notebook-no-direct-accesso a internet	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	lambda-function-public-access-proibito	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	redshift-cluster-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	rds-instance-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	ec2- instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	blocchi s-3 account-level-public-access	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	s3- bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	sagemaker-notebook-no-direct-accesso a Internet	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	vpc-default-security-group-chiuso	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	s3- bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	ec2- instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	ebs-snapshot-public-restorable-controlla	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-4	Il sistema informativo applica le autorizzazioni approvate per il controllo del flusso di informazioni all'interno del sistema e tra sistemi interconnessi in base a [Assegnazione: policy di controllo del flusso di informazioni definite dall'organizzazione].	internet-gateway-authorized-vpc-solo	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			e altre informazioni amministrative su ogni principale.
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-group-has-users-controlla	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-5c	L'organizzazione: c. Definisce le autorizzazioni di accesso al sistema informativo per supportare la separazione dei compiti.	iam-user-no-policies-controlla	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	rds-instance-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	redshift-cluster-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	blocchi s3 account-level-public-access	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	s3- bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	s3- bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	s3- bucket-public-writ e-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	sagemaker-notebook -no-direct-accesso a Internet	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	lambda-function-pu blic-access-proibito	Gestisci l'accesso alle risorse nel AWS Cloud assicuran do che le funzioni AWS Lambda non siano accessibi li pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	codebuild-project-envvar-awscred-controlla	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	ebs-snapshot-public-restorable-controlla	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	iam-user-unused-credentials-controlla	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			e altre informazioni amministrative su ogni principale.
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	iam-group-has-users-controlla	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	iam-root-access-key-controlla	L'accesso ai sistemi e agli asset può essere controllato controlla ndo che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	iam-user-group-membership-controlla	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizzative e alle funzioni aziendali.	iam-user-no-policies-controlla	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	ec2- instance-no-public-ip	Gestisci l'accesso al AWS cloud assicuran do che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6	L'organizzazione utilizza il principio del privilegio minimo, che consente accessi autorizzati solo agli utenti (o ai processi che agiscono per conto degli utenti) necessari per svolgere le attività assegnate in conformità alle missioni organizza tive e alle funzioni aziendali.	iam-no-inline-policy-controlla	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-6(10)	Il sistema informativo impedisce agli utenti non privilegiati di eseguire funzioni privilegiate, tra cui la disabilitazione, l'elusione o la modifica delle protezioni/contromisure di sicurezza implementate.	iam-root-access-key-controlla	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-17(1)	Il sistema informativo monitora e controlla i metodi di accesso remoto.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
AC-17(2)	Il sistema informati vo implementa meccanismi crittogra fici per proteggere la riservatezza e l'integri tà delle sessioni di accesso remoto.	alb-http-to-https-controllo del reindiriz zamento	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-17(2)	Il sistema informativo implementa meccanismi crittografici per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC-17(2)	Il sistema informativo implementa meccanismi crittografici per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto.	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-17(2)	Il sistema informativo implementa meccanismi crittografici per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto.	s-3 bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC-17(2)	Il sistema informativo implementa meccanismi crittografici per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-17(2)	Il sistema informativo implementa meccanismi crittografici per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto.	alb-http-drop-invalid-abilitato per gli header	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC-17(2)	Il sistema informativo implementa meccanismi crittografici per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto.	elb-tls-https-listeners-solo	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-17(3)	Il sistema informativo indirizza tutti gli accessi remoti attraverso [Assegnazione: numero definito dall'organizzazione] punti di controllo di accesso alla rete gestiti.	internet-gateway-authorized-vpc-solo	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	ebs-snapshot-public-restorable-controlla	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	ec2- instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	lambda-function-public-access-proibito	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	rds-instance-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	redshift-cluster-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	blocchi s3 account-level-public-access	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	s3- bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	s3- bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AC-21(b)	L'organizzazione: b. Impiega [Assegnazione: meccanismi automatizzati o processi manuali definiti dall'organizzazione] per assistere gli utenti nel prendere decisioni relative alla condivisione delle informazioni e alla collaborazione.	sagemaker-notebook-no-direct-accesso a Internet	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-2(a)(d)	L'organizzazione: a. Determina che il sistema informativo è in grado di controlla re i seguenti eventi: [Assegnazione: eventi verificabili definiti dall'organizzazion e]; d. Determina che i seguenti eventi devono essere verificati all'interno del sistema informati vo: [Assegnazione: eventi verificati definiti dall'organizzazion e (il sottoinsieme degli eventi verificab ili definiti in AU-2 a.) insieme alla frequenza di verifica (o alla situazione che la richiede) per ogni evento identificato].	api-gw-execution-l ogging-abilitato	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-2(a)(d)	L'organizzazione: a. Determina che il sistema informativo è in grado di controlla re i seguenti eventi: [Assegnazione: eventi verificabili definiti dall'organizzazion e]; d. Determina che i seguenti eventi devono essere verificati all'interno del sistema informati vo: [Assegnazione: eventi verificati definiti dall'organizzazion e (il sottoinsieme degli eventi verificab ili definiti in AU-2 a.) insieme alla frequenza di verifica (o alla situazione che la richiede) per ogni evento identificato].	cloud-trail-cloud-watch-abilitato ai registri	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-2(a)(d)	L'organizzazione: a. Determina che il sistema informativo è in grado di controlla re i seguenti eventi: [Assegnazione: eventi verificabili definiti dall'organizzazion e]; d. Determina che i seguenti eventi devono essere verificati all'interno del sistema informati vo: [Assegnazione: eventi verificati definiti dall'organizzazion e (il sottoinsieme degli eventi verificab ili definiti in AU-2 a.) insieme alla frequenza di verifica (o alla situazione che la richiede) per ogni evento identificato].	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli Account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-2(a)(d)	L'organizzazione: a. Determina che il sistema informativo è in grado di controlla re i seguenti eventi: [Assegnazione: eventi verificabili definiti dall'organizzazion e]; d. Determina che i seguenti eventi devono essere verificati all'interno del sistema informati vo: [Assegnazione: eventi verificati definiti dall'organizzazion e (il sottoinsieme degli eventi verificab ili definiti in AU-2 a.) insieme alla frequenza di verifica (o alla situazione che la richiede) per ogni evento identificato].	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-2(a)(d)	L'organizzazione: a. Determina che il sistema informativo è in grado di controlla re i seguenti eventi: [Assegnazione: eventi verificabili definiti dall'organizzazion e]; d. Determina che i seguenti eventi devono essere verificati all'interno del sistema informati vo: [Assegnazione: eventi verificati definiti dall'organizzazion e (il sottoinsieme degli eventi verificab ili definiti in AU-2 a.) insieme alla frequenza di verifica (o alla situazione che la richiede) per ogni evento identificato].	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicaz ione centrale all'inter no di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettaglia te sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-2(a)(d)	L'organizzazione: a. Determina che il sistema informativo è in grado di controlla re i seguenti eventi: [Assegnazione: eventi verificabili definiti dall'organizzazion e]; d. Determina che i seguenti eventi devono essere verificati all'interno del sistema informati vo: [Assegnazione: eventi verificati definiti dall'organizzazion e (il sottoinsieme degli eventi verificab ili definiti in AU-2 a.) insieme alla frequenza di verifica (o alla situazione che la richiede) per ogni evento identificato].	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail invierà i file di registro da tutti Regioni AWS al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS lancia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-2(a)(d)	L'organizzazione: a. Determina che il sistema informativo è in grado di controlla re i seguenti eventi: [Assegnazione: eventi verificabili definiti dall'organizzazion e]; d. Determina che i seguenti eventi devono essere verificati all'interno del sistema informati vo: [Assegnazione: eventi verificati definiti dall'organizzazion e (il sottoinsieme degli eventi verificab ili definiti in AU-2 a.) insieme alla frequenza di verifica (o alla situazione che la richiede) per ogni evento identificato].	s3- bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-2(a)(d)	L'organizzazione: a. Determina che il sistema informativo è in grado di controlla re i seguenti eventi: [Assegnazione: eventi verificabili definiti dall'organizzazion e]; d. Determina che i seguenti eventi devono essere verificati all'interno del sistema informati vo: [Assegnazione: eventi verificati definiti dall'organizzazion e (il sottoinsieme degli eventi verificab ili definiti in AU-2 a.) insieme alla frequenza di verifica (o alla situazione che la richiede) per ogni evento identificato].	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-2(a)(d)	L'organizzazione: a. Determina che il sistema informativo è in grado di controlla re i seguenti eventi: [Assegnazione: eventi verificabili definiti dall'organizzazion e]; d. Determina che i seguenti eventi devono essere verificati all'interno del sistema informati vo: [Assegnazione: eventi verificati definiti dall'organizzazion e (il sottoinsieme degli eventi verificab ili definiti in AU-2 a.) insieme alla frequenza di verifica (o alla situazione che la richiede) per ogni evento identificato].	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-2(a)(d)	L'organizzazione: a. Determina che il sistema informativo è in grado di controlla re i seguenti eventi: [Assegnazione: eventi verificabili definiti dall'organizzazion e]; d. Determina che i seguenti eventi devono essere verificati all'interno del sistema informati vo: [Assegnazione: eventi verificati definiti dall'organizzazion e (il sottoinsieme degli eventi verificab ili definiti in AU-2 a.) insieme alla frequenza di verifica (o alla situazione che la richiede) per ogni evento identificato].	wafv2-logging-enab led	Per facilitare la registrazione e il monitoraggio all'inter no del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispon dente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-2(a)(d)	L'organizzazione: a. Determina che il sistema informativo è in grado di controlla re i seguenti eventi: [Assegnazione: eventi verificabili definiti dall'organizzazion e]; d. Determina che i seguenti eventi devono essere verificati all'interno del sistema informati vo: [Assegnazione: eventi verificati definiti dall'organizzazion e (il sottoinsieme degli eventi verificab ili definiti in AU-2 a.) insieme alla frequenza di verifica (o alla situazione che la richiede) per ogni evento identificato].	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	api-gw-execution-logging-abilitato	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	cloud-trail-cloud-watch-abilitato ai registri	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli Account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail invierà i file di registro da tutti Regioni AWS al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS lancia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	s3- bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-3	Il sistema informativo genera record di verifica contenenti informazioni che definiscono il tipo di evento che si è verificato, quando e dove si è verificato, la sua origine, il suo esito e l'identità di eventuali persone o soggetti associati all'evento.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-6(1)(3)	(1) L'organizzazione utilizza meccanism i automatizzati per integrare i processi di revisione, analisi e creazione di report di audit a supporto dei processi organizza tivi di indagine sulle attività sospette e di risposta alle stesse. (3) L'organiz zazione analizza e mette in correlazi one i record di audit in diversi repositor y per acquisire una conoscenza della situazione a livello di organizzazione.	cloud-trail-cloud-watch-abilitato ai registri	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-7(1)	Il sistema informativo offre la capacità di elaborare record di audit per eventi di interesse sulla base di [Assegnazione: campi di audit definiti dall'organizzazione all'interno dei record di audit].	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-7(1)	Il sistema informativo offre la capacità di elaborare record di audit per eventi di interesse sulla base di [Assegnazione: campi di audit definiti dall'organizzazione all'interno dei record di audit].	cloud-trail-cloud-watch-abilitato ai registri	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
AU-9	Il sistema informativo protegge le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
AU-9	Il sistema informativo protegge le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-9(2)	Il sistema informativo esegue il backup dei record di verifica [Assegnazione: frequenza definita dall'organizzazione] su un sistema o componente di sistema fisicamente diverso rispetto al sistema o al componente sottoposto a verifica.	s-3 bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
AU-11	L'organizzazione conserva i registri di controllo per [Incarico: periodo di tempo definito dall'organizzazione in conformità con la politica di conservazione dei record] per fornire supporto after-the-fact nelle indagini sugli incidenti di sicurezza e per soddisfare i requisiti normativi e organizzativi di conservazione delle informazioni.	cw-loggroup-retention-period-controlla	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Offre la capacità di generare record di verifica per gli eventi verificabili definiti in AU-2 a. in [Assegnazione: componenti del sistema informativo definiti dall'organizzazione]; c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	api-gw-execution-logging-abilitato	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
AU-12(a)(c)	Il sistema informativo: a. Offre la capacità di generare record di verifica per gli eventi verificabili definiti in AU-2 a. in [Assegnazione: componenti del sistema informativo definiti dall'organizzazione]; c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	cloud-trail-cloud-watch-abilitato ai registri	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Offre la capacità di generare record di verifica per gli eventi verificabili definiti in AU-2 a. in [Assegnazione: componenti del sistema informativo definiti dall'organizzazione]; c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli Account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU-12(a)(c)	Il sistema informativo: a. Offre la capacità di generare record di verifica per gli eventi verificabili definiti in AU-2 a. in [Assegnazione: componenti del sistema informativo definiti dall'organizzazione]; c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Offre la capacità di generare record di verifica per gli eventi verificabili definiti in AU-2 a. in [Assegnazione: componenti del sistema informativo definiti dall'organizzazione]; c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Offre la capacità di generare record di verifica per gli eventi verificabili definiti in AU-2 a. in [Assegnazione: componenti del sistema informativo definiti dall'organizzazione]; c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Offre la capacità di generare record di verifica per gli eventi verificabili definiti in AU-2 a. in [Assegnazione: componenti del sistema informativo definiti dall'organizzazione]; c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail invierà i file di registro da tutti Regioni AWS al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS lancia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Offre la capacità di generare record di verifica per gli eventi verificabili definiti in AU-2 a. in [Assegnazione: componenti del sistema informativo definiti dall'organizzazione]; c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	s3- bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Offre la capacità di generare record di verifica per gli eventi verificabili definiti in AU-2 a. in [Assegnazione: componenti del sistema informativo definiti dall'organizzazione]; c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Offre la capacità di generare record di verifica per gli eventi verificabili definiti in AU-2 a. in [Assegnazione: componenti del sistema informativo definiti dall'organizzazione]; c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
AU-12(a)(c)	Il sistema informativo: a. Offre la capacità di generare record di verifica per gli eventi verificabili definiti in AU-2 a. in [Assegnazione: componenti del sistema informativo definiti dall'organizzazione]; c. Genera record di verifica per gli eventi definiti in AU-2 d. con il contenuto definito in AU-3.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	cloud-trail-cloud-watch-abilitato per i log	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	ec2- instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitorag gio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CA-7(a)(b)	L'organizzazione sviluppa una strategia di monitoraggio continuo e implement a un programma di monitoraggio continuo che include: a. Istituzione di [Assegnazione: metriche definite dall'organizzazion e] da monitorar e; b. Istituzione di [Assegnazione: frequenze definite dall'organizzazion e] per il monitorag gio e [Assegnazione: frequenze definite dall'organizzazion e] per le valutazio ni a supporto di tale monitoraggio.	rds-enhanced-monit oring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorar e la disponibilità di Amazon RDS. Ciò fornisce una visibilit à dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archivi azione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositi vo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	ec2- -gestore instance-managed-by-systems	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	ec2- -controllamanagedinstance-association-compliance-status	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	ec2- volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-2	L'organizzazione sviluppa, documenta e mantiene sotto il controllo della configurazione una configurazione di base corrente del sistema informativo.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-7(a)	L'organizzazione: a. Configura il sistema informativo per fornire solo le funzionalità essenziali.	ec2- -manager instance-managed-by-systems	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-7(a)	L'organizzazione: a. Configura il sistema informativo per fornire solo le funzionalità essenziali.	ec2- -controllamanagedinstance-association-compliance-status	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-8(1)	L'organizzazione aggiorna l'inventario dei componenti del sistema informativo come parte integrant e delle installazioni dei componenti, delle rimozioni e degli aggiornamenti del sistema stesso.	ec2- -manager instance-managed-by-systems	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-8(3)(a)	L'organizzazione: a. Utilizza meccanism i automatizzati [Assegnazione: frequenza definita dall'organizzazion e] per rilevare la presenza di componenti hardware, software e firmware non autorizzati all'interno del sistema informativo.	ec2- -manager instance-managed-by-systems	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-8(3)(a)	L'organizzazione: a. Utilizza meccanismi automatizzati [Assegnazione: frequenza definita dall'organizzazione] per rilevare la presenza di componenti hardware, software e firmware non autorizzati all'interno del sistema informativo.	ec2- -controllamanagedinstance-association-compliance-status	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CM-8(3)(a)	L'organizzazione: a. Utilizza meccanismi automatizzati [Assegnazione: frequenza definita dall'organizzazione] per rilevare la presenza di componenti hardware, software e firmware non autorizzati all'interno del sistema informativo.	ec2- -controllamanagedinstance-patch-compliance-status	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-9(b)	L'organizzazione: b. Esegue il backup delle informazioni a livello di sistema contenute nel sistema informativo [Assegnazione: frequenza definita dall'organizzazione coerente con gli obiettivi del tempo di ripristino e del punto di ripristino].	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
CP-9(b)	L'organizzazione: b. Esegue il backup delle informazioni a livello di sistema contenute nel sistema informativo [Assegnazione: frequenza definita dall'organizzazione coerente con gli obiettivi del tempo di ripristino e del punto di ripristino].	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-9(b)	L'organizzazione: b. Esegue il backup delle informazioni a livello di sistema contenute nel sistema informativo [Assegnazione: frequenza definita dall'organizzazione coerente con gli obiettivi del tempo di ripristino e del punto di ripristino].	elasticache-redis-cluster-automatic-controllo del backup	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-9(b)	L'organizzazione: b. Esegue il backup delle informazioni a livello di sistema contenute nel sistema informativo [Assegnazione: frequenza definita dall'organizzazione coerente con gli obiettivi del tempo di ripristino e del punto di ripristino].	s-3 bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-9(b)	L'organizzazione: b. Esegue il backup delle informazioni a livello di sistema contenute nel sistema informativo [Assegnazione: frequenza definita dall'organizzazione coerente con gli obiettivi del tempo di ripristino e del punto di ripristino].	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-9(b)	L'organizzazione: b. Esegue il backup delle informazioni a livello di sistema contenute nel sistema informativo [Assegnazione: frequenza definita dall'organizzazione coerente con gli obiettivi del tempo di ripristino e del punto di ripristino].	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-9(b)	L'organizzazione: b. Esegue il backup delle informazioni a livello di sistema contenute nel sistema informativo [Assegnazione: frequenza definita dall'organizzazione coerente con gli obiettivi del tempo di ripristino e del punto di ripristino].	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-9(b)	L'organizzazione: b. Esegue il backup delle informazioni a livello di sistema contenute nel sistema informativo [Assegnazione: frequenza definita dall'organizzazione coerente con gli obiettivi del tempo di ripristino e del punto di ripristino].	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			e le operazioni del database non appena il failover è completato.
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	s3- bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	elasticache-redis-cluster-automatic-controllo del backup	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	s-3 bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	elb-cross-zone-load-abilitato al bilanciamento	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
CP-10	L'organizzazione provvede al ripristino e alla ricostituzione del sistema informativo a uno stato noto dopo un'interruzione, una compromissione o un guasto.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
IA-2	Il sistema informativo identifica e autentica in modo univoco gli utenti dell'orga nizzazione (o i processi che agiscono per loro conto).	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazion e. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dal Centers for Internet Security (CIS) AWS Foundatio ns Benchmark per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foun dational Security Best Practices value: true), RequireSy mbols (AWS Foun dational Security Best Practices value: true), RequireNu mbers (AWS Foun

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			dational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
IA-2(1)(11)	(1) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account con privilegi. (11) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso remoto negli account con e senza privilegi, in modo che uno dei fattori sia fornito da un dispositivo diverso dal sistema che ottiene l'accesso e che il dispositivo soddisfi [Assegnazione: requisiti di affidabilità del meccanismo definiti dall'organizzazione].	root-account-hardware-mfa-abilitato	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
IA-2(1)(11)	(1) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account con privilegi. (11) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso remoto negli account con e senza privilegi, in modo che uno dei fattori sia fornito da un dispositivo diverso dal sistema che ottiene l'accesso e che il dispositivo soddisfi [Assegnazione: requisiti di affidabilità del meccanismo definiti dall'organizzazione].	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
IA-2(1)(2)(11)	(1) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account con privilegi. (2) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account senza privilegi. (11) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso remoto negli account con e senza privilegi, in modo che uno dei fattori sia fornito da un dispositivo diverso dal sistema che ottiene l'accesso e che il dispositivo soddisfi [Assegnazione: requisiti di affidabilità del meccanismo definiti dall'organizzazione].	mfa-enabled-for-iam-accesso alla console	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione e alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
IA-2(1)(2)(11)	(1) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account con privilegi. (2) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso alla rete negli account senza privilegi. (11) Il sistema informativo implementa l'autenticazione a più fattori per l'accesso remoto negli account con e senza privilegi, in modo che uno dei fattori sia fornito da un dispositivo diverso dal sistema che ottiene l'accesso e che il dispositivo soddisfi [Assegnazione: requisiti di affidabilità del meccanismo definiti dall'organizzazione].	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
IA-5(1)(a)(d)(e)	Il sistema informativo, per l'autenticazione basata su password: a. Applica una complessità minima della password di [Assegnazione: requisiti definiti dall'organizzazion e per la distinzio ne tra maiuscole e minuscole, numero di caratteri, combinazi one di lettere maiuscole, lettere minuscole, numeri e caratteri speciali, inclusi i requisiti minimi per ogni tipo]; d. Applica le restrizioni sulla durata minima e massima delle password di [Assegnazione: numeri definiti dall'organizzazione per la durata minima, durata massima]; e. Proibisce il riutilizz o della password per [Assegnazione: numero definito	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti indicati dal NIST SP 800-63 e dal benchmark Centers for Internet Security (CIS) AWS Foundations per quanto riguarda la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foun dational Security Best Practices value: true), RequireSy mbols (AWS Foun dational Security Best Practices value: true), RequireNu

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	dall'organizzazione] generazioni.		mbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
IA-5(4)	L'organizzazione utilizza strumenti automatizzati per determinare se gli autenticatori di password sono sufficientemente potenti da soddisfare [Assegnazione: requisiti definiti dall'organizzazione].	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dal Centers for Internet Security (CIS) AWS Foundations Benchmark per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foun

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			dational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
IA-5(7)	L'organizzazione garantisce che gli autenticatori statici non crittografati non vengano incorporati nelle applicazioni o negli script di accesso o memorizzati nei tasti funzione.	codebuild-project-envvar-awscred-controlla	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
IR-4(1)	L'organizzazione utilizza meccanism i automatizzati per supportare il processo di gestione degli incidenti.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
IR-4(1)	L'organizzazione utilizza meccanismi automatizzati per supportare il processo di gestione degli incidenti.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
IR-6(1)	L'organizzazione utilizza meccanismi automatizzati per facilitare la segnalazione degli incidenti di sicurezza.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
IR-7(1)	L'organizzazione utilizza meccanismi automatizzati per aumentare la disponibilità di informazioni e supporto relativi alla risposta agli incidenti.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
RA-5	L'organizzazione: a. Esegue la scansione delle vulnerabilità nel sistema informativo e nelle applicazioni ospitate [Assegnazione: frequenza definita dall'organizzazione e/o in modo casuale in base al processo definito dall'organizzazione] e quando vengono identificate e segnalate nuove vulnerabilità che potrebbero influire sul sistema/sulle applicazioni; b. Utilizza strumenti e tecniche di scansione delle vulnerabilità che facilitano l'interoperabilità tra gli strumenti e automatizzano parti del processo di gestione delle vulnerabilità utilizzando standard per: 1. Enumerazione di piattaforme, difetti del software e configura	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	zioni improprie; 2. Formattazione di liste di controllo e procedure di test; e 3. Misurazione dell'impatto delle vulnerabilità; c. Analizza i report di scansione delle vulnerabilità e i risultati delle valutazioni del controllo di sicurezza; d. Corregge le vulnerabilità legittime [Assegnazione: tempi di risposta definiti dall'organizzazione], secondo una valutazione del rischio dell'organizzazione; e. Condivide le informazioni ottenute dal processo di scansione delle vulnerabilità e dalle valutazioni del controllo della sicurezza con [Assegnazione: personale o ruoli definiti dall'organizzazione] per aiutare a eliminare vulnerabilità simili in altri sistemi informativi		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	(ad esempio, criticità o carenze sistemiche).		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
RA-5	L'organizzazione: a. Esegue la scansione delle vulnerabilità nel sistema informativo e nelle applicazioni ospitate [Assegnazione: frequenza definita dall'organizzazione e/o in modo casuale in base al processo definito dall'organizzazione] e quando vengono identificate e segnalate nuove vulnerabilità che potrebbero influire sul sistema/sulle applicazioni; b. Utilizza strumenti e tecniche di scansione delle vulnerabilità che facilitano l'interoperabilità tra gli strumenti e automatizzano parti del processo di gestione delle vulnerabilità utilizzando standard per: 1. Enumerazione di piattaforme, difetti del software e configura	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	zioni improprie; 2. Formattazione di liste di controllo e procedure di test; e 3. Misurazione dell'impatto delle vulnerabilità; c. Analizza i report di scansione delle vulnerabilità e i risultati delle valutazioni del controllo di sicurezza; d. Corregge le vulnerabilità legittime [Assegnazione: tempi di risposta definiti dall'organizzazione], secondo una valutazione del rischio dell'organizzazione; e. Condivide le informazioni ottenute dal processo di scansione delle vulnerabilità e dalle valutazioni del controllo della sicurezza con [Assegnazione: personale o ruoli definiti dall'organizzazione] per aiutare a eliminare vulnerabilità simili in altri sistemi informativi		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	(ad esempio, criticità o carenze sistemiche).		
SA-3(a)	L'organizzazione: a. Gestisce il sistema informativo utilizzando [Assegnazione: ciclo di vita dello sviluppo del sistema definito dall'organizzazione] che incorpora considerazioni sulla sicurezza delle informazioni.	codebuild-project-envvar-awscred-controlla	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SA-3(a)	L'organizzazione: a. Gestisce il sistema informativo utilizzando [Assegnazione: ciclo di vita dello sviluppo del sistema definito dall'organizzazione] che incorpora considerazioni sulla sicurezza delle informazioni.	instance-managed-by-systemsec2- -manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SA-3(a)	L'organizzazione: a. Gestisce il sistema informativo utilizzando [Assegnazione: ciclo di vita dello sviluppo del sistema definito dall'organizzazione] che incorpora considerazioni sulla sicurezza delle informazioni.	codebuild-project-source-repo-controllo dell'URL	Assicurati che l' GitHub URL del repository di origine di Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SA-10	L'organizzazione richiede allo sviluppatore del sistema informativo, del componente del sistema o del servizio del sistema informativo di: a. Gestire la configurazione durante [Selezione (una o più): la progettazione; lo sviluppo; l'implementazione; il funzionamento] del sistema, del componente o del servizio; b. Documentare, gestire e controllare l'integrità delle modifiche a [Assegnazione: elementi di configurazione definiti dall'organizzazione nell'ambito della gestione della configurazione]; c. Implementare solo le modifiche al sistema, al componente o al servizio approvate dall'organizzazione; d. Documentare le modifiche al sistema,	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	al componente o al servizio approvate e i potenziali impatti sulla sicurezza di tali modifiche; e. Tieni traccia dei difetti di sicurezza e della risoluzione dei difetti all'interno del sistema, del componente o del servizio e segnala i risultati a [Assegnazione: personale definito dall'organizzazione].		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SA-10	L'organizzazione richiede allo sviluppatore del sistema informativo, del componente del sistema o del servizio del sistema informativo di: a. Gestire la configurazione durante [Selezione (una o più): la progettazione; lo sviluppo; l'implementazione; il funzionamento] del sistema, del componente o del servizio; b. Documentare, gestire e controllare l'integrità delle modifiche a [Assegnazione: elementi di configurazione definiti dall'organizzazione nell'ambito della gestione della configurazione]; c. Implementare solo le modifiche al sistema, al componente o al servizio approvate dall'organizzazione; d. Documentare le modifiche al sistema,	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	al componente o al servizio approvate e i potenziali impatti sulla sicurezza di tali modifiche; e. Tieni traccia dei difetti di sicurezza e della risoluzione dei difetti all'interno del sistema, del componente o del servizio e segnala i risultati a [Assegnazione: personale definito dall'organizzazione].		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SA-10	L'organizzazione richiede allo sviluppatore del sistema informativo, del componente del sistema o del servizio del sistema informativo di: a. Gestire la configurazione durante [Selezione (una o più): la progettazione; lo sviluppo; l'implementazione; il funzionamento] del sistema, del componente o del servizio; b. Documentare, gestire e controllare l'integrità delle modifiche a [Assegnazione: elementi di configurazione definiti dall'organizzazione nell'ambito della gestione della configurazione]; c. Implementare solo le modifiche al sistema, al componente o al servizio approvate dall'organizzazione; d. Documentare le modifiche al sistema,	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	al componente o al servizio approvate e i potenziali impatti sulla sicurezza di tali modifiche; e. Tieni traccia dei difetti di sicurezza e della risoluzione dei difetti all'interno del sistema, del componente o del servizio e segnala i risultati a [Assegnazione: personale definito dall'organizzazione].		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SA-10	L'organizzazione richiede allo sviluppatore del sistema informativo, del componente del sistema o del servizio del sistema informativo di: a. Gestire la configurazione durante [Selezione (una o più): la progettazione; lo sviluppo; l'implementazione; il funzionamento] del sistema, del componente o del servizio; b. Documentare, gestire e controllare l'integrità delle modifiche a [Assegnazione: elementi di configurazione definiti dall'organizzazione nell'ambito della gestione della configurazione]; c. Implementare solo le modifiche al sistema, al componente o al servizio approvate dall'organizzazione; d. Documentare le modifiche al sistema,	ec2- -manager instance-managed-by-systems	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	al componente o al servizio approvate e i potenziali impatti sulla sicurezza di tali modifiche; e. Tieni traccia dei difetti di sicurezza e della risoluzione dei difetti all'interno del sistema, del componente o del servizio e segnala i risultati a [Assegnazione: personale definito dall'organizzazione].		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-2	Il sistema informativo separa la funzionalità utente (compresi i servizi di interfaccia utente) dalla funzionalità di gestione del sistema informativo.	iam-group-has-users-controlla	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-2	Il sistema informativo separa la funzionalità utente (compresi i servizi di interfaccia utente) dalla funzionalità di gestione del sistema informativo.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-4	Il sistema informativo impedisce il trasferimento non autorizzato e non intenzionale di informazioni attraverso le risorse di sistema condivise.	ec2- volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	autoscaling-group-elb-healthcheck-richiesto	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			e le operazioni del database non appena il failover è completato.
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	s3- bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	elb-cross-zone-load-abilitato al bilanciamento	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-5	Il sistema informativo protegge dai seguenti tipi di attacchi Denial of Service o ne limita gli effetti: [Assegnazione: tipi di attacchi Denial of Service definiti dall'organizzazione o riferimenti alle fonti di tali informazioni] utilizzando [Assegnazione: misure di sicurezza definite dall'organizzazione].	rds-instance-deletion-protection-abilitato	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	ec2- instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	s3- bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	alb-http-to-https-controllo del reindirizzamento	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	elb-tls-https-listeners-solo	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	ec2- instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	internet-gateway-authorized-vpc-solo	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	ebs-snapshot-public-restorable-controlla	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	lambda-function-public-access-proibito	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	rds-instance-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	redshift-cluster-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	s3- bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	s3- bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	sagemaker-notebook-no-direct-accesso a Internet	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	vpc-default-security-group-chiuso	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	s-3 bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	blocchi s3 account-level-public-access	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	alb-http-drop-invalid-abilitato per gli header	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7	Il sistema informativo: a. Monitora e controlla le comunicazioni ai confini esterni e ai principali confini interni del sistema; b. Implementa sottoreti per componenti di sistema accessibili pubblicamente che sono [Selezione: fisicamente; logicamente] separati dalle reti interne dell'organizzazione; c. Si connette a reti o sistemi informativi esterni solo tramite interfacce gestite costituite da dispositivi di protezione dei confini disposti secondo un'architettura di sicurezza dell'organizzazione.	elasticsearch-node-to-node-controllo della crittografia	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	ec2- instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	internet-gateway-authorized-vpc-solo	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	ebs-snapshot-public-restorable-controlla	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	ec2- instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	lambda-function-public-access-proibito	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	rds-instance-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	redshift-cluster-public-access-controlla	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	blocchi s3 account-level-public-access	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	s3- bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	s3- bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	s3- bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	sagemaker-notebook-no-direct-accesso a Internet	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	vpc-default-security-group-chiuso	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-7(3)	L'organizzazione limita il numero di connessioni di rete esterne al sistema informativo.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-8	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] delle informazioni trasmesse.	alb-http-to-https-controllo del reindirizzamento	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] delle informazioni trasmesse.	alb-http-drop-invalid-abilitato per gli header	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-8	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] delle informazioni trasmesse.	elasticsearch-node-to-node-controllo della crittografia	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] delle informazioni trasmesse.	elb-tls-https-listeners-solo	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-8	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] delle informazioni trasmesse.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] delle informazioni trasmesse.	s3- bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-8	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] delle informazioni trasmesse.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	alb-http-to-https-controllo del reindirizzamento	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	alb-http-drop-invalid-abilitato per gli header	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	elasticsearch-node-to-node-controllo della crittografia	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	elb-tls-https-listeners-solo	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	s3- bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-8(1)	Il sistema informativo implementa meccanismi crittografici per [Selezione (una o più): impedire la divulgazione non autorizzata di informazioni; rilevare le modifiche alle informazioni] durante la trasmissione, a meno che non sia diversamente protetto da [Assegnazione: protezioni fisiche alternative definite dall'organizzazione].	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-12	L'organizzazione stabilisce e gestisce le chiavi crittografiche per la crittografia richiesta impiegata all'interno del sistema informativo in conformità a [Assegnazione: requisiti definiti dall'organizzazione per la generazione, la distribuzione, l'archiviazione e la distruzione delle chiavi e l'accesso alle stesse].	cmk-backing-key-rotation-abilitato	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-12	L'organizzazione stabilisce e gestisce le chiavi crittografiche per la crittografia richiesta impiegata all'interno del sistema informativo in conformità a [Assegnazione: requisiti definiti dall'organizzazione per la generazione, la distribuzione, l'archiviazione e la distruzione delle chiavi e l'accesso alle stesse].	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-12	L'organizzazione stabilisce e gestisce le chiavi crittografiche per la crittografia richiesta impiegata all'interno del sistema informativo in conformità a [Assegnazione: requisiti definiti dall'organizzazione per la generazione, la distribuzione, l'archiviazione e la distruzione delle chiavi e l'accesso alle stesse].	kms-cmk-not-scheduled-per la cancellazione	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (KMS).AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	alb-http-to-https-controllo del reindirizzamento	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	api-gw-cache-enabled-e crittografato	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	abilitato a s3 bucket-server-side-encryption	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	s3- bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	sagemaker-endpoint-configuration-kms-configurato a chiave	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	sagemaker-notebook-instance-kms-configurato con chiave	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-13	Il sistema informativo implementa [Assegnazione: usi crittografici definiti dall'organizzazione e tipo di crittografia richiesta per ciascun utilizzo] in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-13	Il sistema informativo implementa la crittografia convalidata da FIPS o approvata da NSA in conformità alle leggi federali applicabili, agli ordini esecutivi, alle direttive, alle policy, ai regolamenti e agli standard.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
SC-23	Il sistema informativo protegge l'autenticità delle sessioni di comunicazione.	alb-http-to-https-controllo del reindirizzamento	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-23	Il sistema informativo protegge l'autenticità delle sessioni di comunicazione.	alb-http-drop-invalid-abilitato per gli header	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-23	Il sistema informativo protegge l'autenticità delle sessioni di comunicazione.	elb-tls-https-listeners-solo	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	api-gw-cache-enabled-e crittografato	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	kms-cmk-not-scheduled-per la cancellazione	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (KMS).AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	s3- bucket-default-lock-enabled	Assicurati che il blocco sia abilitato , per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	abilitato a s3 bucket-server-side-encryption	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	sagemaker-endpoint-configuration-kms-configurato con chiave	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	sagemaker-notebook-instance-kms-configurato con chiave	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	ec2- ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
SC-28	Il sistema informativo protegge [Selezione (una o più): la riservatezza; l'integrità] di [Assegnazione: informazioni a riposo definite dall'organizzazione].	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SC-36	L'organizzazione distribuisce [Assegnazione: elaborazione e archiviazione definiti dall'organizzazione] tra più posizioni fisiche.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
			e le operazioni del database non appena il failover è completato.
SC-36	L'organizzazione distribuisce [Assegnazione: elaborazione e archiviazione definiti dall'organizzazione] tra più posizioni fisiche.	s3- bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-2(2)	L'organizzazione utilizza meccanismi automatizzati [Assegnazione: frequenza definita dall'organizzazione] per determinare lo stato dei componenti del sistema informativo per quanto riguarda la correzione dei difetti.	ec2- -controllamanagedinstance-patch-compliance-status	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-2(2)	L'organizzazione utilizza meccanism i automatizzati [Assegnazione: frequenza definita dall'organizzazione] per determinare lo stato dei componenti del sistema informati vo per quanto riguarda la correzione dei difetti.	ec2- -manager instance-managed-by-systems	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-2(2)	L'organizzazione utilizza meccanismi automatizzati [Assegnazione: frequenza definita dall'organizzazione] per determinare lo stato dei componenti del sistema informativo per quanto riguarda la correzione dei difetti.	ec2- -controllamanagedinstance-association-compliance-status	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(1)	L'organizzazione collega e configura i singoli strumenti di rilevamento delle intrusioni in un sistema di rilevamento delle intrusioni a livello di sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	cloud-trail-cloud-watch-abilitato ai registri	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
SI-4(2)	L'organizzazione utilizza strumenti automatizzati per supportare l'analisi quasi in tempo reale degli eventi.	ec2- instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitorag gio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(4)	Il sistema informativo monitora il traffico di comunicazioni in entrata e in uscita [Assegnazione: frequenza definita dall'organizzazione] per attività o condizioni insolite o non autorizzate.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(4)	Il sistema informativo monitora il traffico di comunicazioni in entrata e in uscita [Assegnazione: frequenza definita dall'organizzazione] per attività o condizioni insolite o non autorizzate.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(4)	Il sistema informativo monitora il traffico di comunicazioni in entrata e in uscita [Assegnazione: frequenza definita dall'organizzazione] per attività o condizioni insolite o non autorizzate.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(4)	Il sistema informativo monitora il traffico di comunicazioni in entrata e in uscita [Assegnazione: frequenza definita dall'organizzazione] per attività o condizioni insolite o non autorizzate.	cloud-trail-cloud-watch-abilitato ai registri	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
SI-4(5)	Il sistema informativo avvisa [Assegnazione: personale o ruoli definiti dall'organizzazione] quando si presentano le seguenti indicazioni di compromissione o potenziale compromissione: [Assegnazione: indicatori di compromissione definiti dall'organizzazione].	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(5)	Il sistema informativo avvisa [Assegnazione: personale o ruoli definiti dall'organizzazione] quando si presentano le seguenti indicazioni di compromissione o potenziale compromissione: [Assegnazione: indicatori di compromissione definiti dall'organizzazione].	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(5)	Il sistema informativo avvisa [Assegnazione: personale o ruoli definiti dall'organizzazione] quando si presentano le seguenti indicazioni di compromissione o potenziale compromissione: [Assegnazione: indicatori di compromissione definiti dall'organizzazione].	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(5)	Il sistema informativo avvisa [Assegnazione: personale o ruoli definiti dall'organizzazione] quando si presentano le seguenti indicazioni di compromissione o potenziale compromissione: [Assegnazione: indicatori di compromissione definiti dall'organizzazione].	cloud-trail-cloud-watch-abilitato ai registri	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
SI-4(16)	L'organizzazione mette in correlazione le informazioni provenienti dagli strumenti di monitoraggio utilizzati in tutto il sistema informativo.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(16)	L'organizzazione mette in correlazi one le informazioni provenienti dagli strumenti di monitorag gio utilizzati in tutto il sistema informativo.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi in conformit à a [Assegnazione: obiettivi di monitorag gio definiti dall'orga nizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnaz ione: tecniche e metodi definiti dall'organizzazion e]; c. Implement a dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazi oni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenziali attacchi in conformità a [Assegnazione: obiettivi di monitoraggio definiti dall'organizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnazione: tecniche e metodi definiti dall'organizzazione]; c. Implementa dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazioni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi in conformit à a [Assegnazione: obiettivi di monitorag gio definiti dall'orga nizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnaz ione: tecniche e metodi definiti dall'organizzazion e]; c. Implement a dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazi oni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenziali attacchi in conformità a [Assegnazione: obiettivi di monitoraggio definiti dall'organizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnazione: tecniche e metodi definiti dall'organizzazione]; c. Implementa dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazioni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi in conformit à a [Assegnazione: obiettivi di monitorag gio definiti dall'orga nizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnaz ione: tecniche e metodi definiti dall'organizzazion e]; c. Implement a dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazi oni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi in conformit à a [Assegnazione: obiettivi di monitorag gio definiti dall'orga nizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnaz ione: tecniche e metodi definiti dall'organizzazion e]; c. Implement a dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazi oni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi in conformit à a [Assegnazione: obiettivi di monitorag gio definiti dall'orga nizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnaz ione: tecniche e metodi definiti dall'organizzazion e]; c. Implement a dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazi oni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	cloud-trail-cloud-watch-abilitato ai registri	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	ni di interesse per l'organizzazione.		

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-4(a)(b)(c)	L'organizzazione: a. Monitora il sistema informativo per rilevare: 1. Attacchi e indicatori di potenzial i attacchi in conformit à a [Assegnazione: obiettivi di monitorag gio definiti dall'orga nizzazione]; 2. Connessioni locali, di rete e remote non autorizzate; b. Identifica l'uso non autorizzato del sistema informativo attraverso [Assegnaz ione: tecniche e metodi definiti dall'organizzazion e]; c. Implement a dispositivi di monitoraggio: i. in modo strategico all'interno del sistema informativo per raccogliere informazi oni essenziali stabilite dall'organizzazione e (ii) in posizioni ad hoc all'interno del sistema per tracciare tipi specifici di transazio	ec2- instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitorag gio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
	ni di interesse per l'organizzazione.		
SI-7	L'organizzazione utilizza strumenti di verifica dell'integrità per rilevare modifiche non autorizzate a [Assegnazione: software, firmware e informazioni definiti dall'organizzazione].	cloud-trail-log-file-abilitato alla convalida	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-7(1)	Il sistema informativo esegue un controllo di integrità su [Assegnazione: software, firmware e informazioni definiti dall'organizzazione] [Selezione (una o più): all'avvio; [Assegnazione: nelle fasi di transizione definite dall'organizzazione o in caso di eventi rilevanti per la sicurezza]; [Assegnazione: frequenza definita dall'organizzazione]].	instance-managed-by-systemsec2- -manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-7(1)	Il sistema informativo esegue un controllo di integrità su [Assegnazione: software, firmware e informazioni definiti dall'organizzazione] [Selezione (una o più): all'avvio; [Assegnazione: nelle fasi di transizione definite dall'organizzazione o in caso di eventi rilevanti per la sicurezza]; [Assegnazione: frequenza definita dall'organizzazione]].	ec2- -controllamanagedinstance-patch-compliance-status	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-7(1)	Il sistema informativo esegue un controllo di integrità su [Assegnazione: software, firmware e informazioni definiti dall'organizzazione] [Selezione (una o più): all'avvio; [Assegnazione: nelle fasi di transizione definite dall'organizzazione o in caso di eventi rilevanti per la sicurezza]; [Assegnazione: frequenza definita dall'organizzazione]].	cloud-trail-log-file-abilitato alla convalida	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	s-3 bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	elasticache-redis-cluster-automatic-controllo del backup	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Config Regola	Linea guida
SI-12	L'organizzazione gestisce e mantiene le informazioni all'interno del sistema e le informazioni in uscita dal sistema in conformità alle leggi, agli ordini esecutivi, alle direttive, ai regolamenti, alle policy, agli standard, alle linee guida e ai requisiti operativi applicabili.	cw-loggroup-retention-period-controlla	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NIST 800-53 rev 4.

Best practice operative per NIST 800-53 rev 5

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il NIST 800-53 e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli NIST 800-53. Un controllo NIST 800-53 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	iam-policy-no-stat ements-with-full-a ccess	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundatio

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			nal Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(1)	Gestione degli account | Gestione automatizzata degli account di sistema	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(3)	Gestione degli account | Disattivazione degli account	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(3)	Gestione degli account | Disattivazione degli account	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(3)	Gestione degli account | Disattivazione degli account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Gestione degli account | Azioni di audit automatizzate	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Gestione degli account | Azioni di audit automatizzate	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Gestione degli account | Azioni di audit automatizzate	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
AC-2(4)	Gestione degli account | Azioni di audit automatizzate	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Gestione degli account | Azioni di audit automatizzate	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
AC-2(4)	Gestione degli account | Azioni di audit automatizzate	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Gestione degli account | Azioni di audit automatizzate	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Gestione degli account | Azioni di audit automatizzate	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(4)	Gestione degli account | Azioni di audit automatizzate	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2(12)	Gestione degli account | Monitoraggio degli account per uso atipico	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	Gestione dell'account	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
AC-2	Gestione dell'account	iam-policy-no-stat ements-with-full-a ccess	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	Gestione dell'account	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	Gestione dell'account	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC-2	Gestione dell'account	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	Gestione dell'account	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-2	Gestione dell'account	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(7)	Applicazione degli accessi | Controllo degli accessi basato sui ruoli	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundatio

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			nal Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3(15)	Applicazione degli accessi | Controllo degli accessi discrezionale e obbligatorio	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.
AC-3	Applicazione degli accessi	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
AC-3	Applicazione degli accessi	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
AC-3	Applicazione degli accessi	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
AC-3	Applicazione degli accessi	iam-policy-no-stat ements-with-full-a ccess	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC-3	Applicazione degli accessi	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-3	Applicazione degli accessi	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC-3	Applicazione degli accessi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-3	Applicazione degli accessi	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC-3	Applicazione degli accessi	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-3	Applicazione degli accessi	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-3	Applicazione degli accessi	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(21)	Applicazione del flusso di informazioni | Separazione fisica o logica dei flussi di informazioni	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicaz ione centrale all'inter no di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettaglia te sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4(26)	Applicazione del flusso di informazioni | Azioni di filtraggio degli audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
AC-4	Applicazione del flusso di informazioni	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC-4	Applicazione del flusso di informazioni	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
AC-4	Applicazione del flusso di informazioni	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
AC-4	Applicazione del flusso di informazioni	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
AC-4	Applicazione del flusso di informazioni	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-4	Applicazione del flusso di informazioni	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
AC-4	Applicazione del flusso di informazioni	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-4	Applicazione del flusso di informazioni	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-4	Applicazione del flusso di informazioni	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
AC-4	Applicazione del flusso di informazioni	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC-4	Applicazione del flusso di informazioni	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-4	Applicazione del flusso di informazioni	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
AC-4	Applicazione del flusso di informazioni	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-4	Applicazione del flusso di informazioni	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5	Separazione dei compiti	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
AC-5	Separazione dei compiti	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5	Separazione dei compiti	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5	Separazione dei compiti	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-5	Separazione dei compiti	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC-5	Separazione dei compiti	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(2)	Privilegio minimo | Accesso senza privilegi per funzioni non legate alla sicurezza	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(2)	Privilegio minimo | Accesso senza privilegi per funzioni non legate alla sicurezza	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(2)	Privilegio minimo | Accesso senza privilegi per funzioni non legate alla sicurezza	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(3)	Privilegio minimo | Accesso alla rete per comandi con privilegi	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
AC-6(3)	Privilegio minimo | Accesso alla rete per comandi con privilegi	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(3)	Privilegio minimo | Accesso alla rete per comandi con privilegi	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(3)	Privilegio minimo | Accesso alla rete per comandi con privilegi	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC-6(3)	Privilegio minimo | Accesso alla rete per comandi con privilegi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(3)	Privilegio minimo | Accesso alla rete per comandi con privilegi	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(9)	Privilegio minimo | Registrazione dell'utilizzo di funzioni con privilegi	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(9)	Privilegio minimo | Registrazione dell'utilizzo di funzioni con privilegi	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(9)	Privilegio minimo | Registrazione dell'utilizzo di funzioni con privilegi	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
AC-6(9)	Privilegio minimo | Registrazione dell'utilizzo di funzioni con privilegi	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(9)	Privilegio minimo | Registrazione dell'utilizzo di funzioni con privilegi	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
AC-6(9)	Privilegio minimo | Registrazione dell'utilizzo di funzioni con privilegi	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(9)	Privilegio minimo | Registrazione dell'utilizzo di funzioni con privilegi	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(9)	Privilegio minimo | Registrazione dell'utilizzo di funzioni con privilegi	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(9)	Privilegio minimo | Registrazione dell'utilizzo di funzioni con privilegi	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(10)	Privilegio minimo | Divieto per gli utenti senza privilegi di eseguire funzioni con privilegi	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(10)	Privilegio minimo | Divieto per gli utenti senza privilegi di eseguire funzioni con privilegi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6(10)	Privilegio minimo | Divieto per gli utenti senza privilegi di eseguire funzioni con privilegi	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
AC-6	Privilegio minimo	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
AC-6	Privilegio minimo	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
AC-6	Privilegio minimo	iam-policy-no-stat ements-with-full-a ccess	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC-6	Privilegio minimo	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-6	Privilegio minimo	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
AC-6	Privilegio minimo	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-6	Privilegio minimo	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC-6	Privilegio minimo	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-6	Privilegio minimo	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-6	Privilegio minimo	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
AC-17(2)	Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(2)	Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC-17(2)	Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
AC-17(2)	Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(2)	Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
AC-17(2)	Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-17(2)	Accesso remoto | Protezione della riservatezza e dell'integrità mediante crittografia	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
AC-21	Condivisione delle informazioni	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
AC-21	Condivisione delle informazioni	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-21	Condivisione delle informazioni	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
AC-21	Condivisione delle informazioni	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
AC-21	Condivisione delle informazioni	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
AC-21	Condivisione delle informazioni	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
AC-21	Condivisione delle informazioni	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AC-21	Condivisione delle informazioni	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	Registrazione degli eventi	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	Registrazione degli eventi	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	Registrazione degli eventi	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	Registrazione degli eventi	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	Registrazione degli eventi	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AU-2	Registrazione degli eventi	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	Registrazione degli eventi	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU-2	Registrazione degli eventi	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	Registrazione degli eventi	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU-2	Registrazione degli eventi	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	Registrazione degli eventi	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	Registrazione degli eventi	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-2	Registrazione degli eventi	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Contenuto dei record di audit	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Contenuto dei record di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Contenuto dei record di audit	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Contenuto dei record di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AU-3	Contenuto dei record di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Contenuto dei record di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU-3	Contenuto dei record di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Contenuto dei record di audit	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU-3	Contenuto dei record di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Contenuto dei record di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Contenuto dei record di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Contenuto dei record di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-3	Contenuto dei record di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
AU-6(1)	Revisione, analisi e reportistica dei record di audit | Integrazione automatizzata dei processi	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)	Revisione, analisi e reportistica dei record di audit | Integrazione automatizzata dei processi	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)	Revisione, analisi e reportistica dei record di audit | Integrazione automatizzata dei processi	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(1)	Revisione, analisi e reportistica dei record di audit | Integrazione automatizzata dei processi	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(3)	Revisione, analisi e reportistica dei record di audit | Correlazione dei repository dei record di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicaz ione centrale all'inter no di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettaglia te sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(4)	Revisione, analisi e reportistica dei record di audit | Revisione e analisi centralizzate	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
AU-6(5)	Revisione, analisi e reportistica dei record di audit | Analisi integrata dei record di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(5)	Revisione, analisi e reportistica dei record di audit | Analisi integrata dei record di audit	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(5)	Revisione, analisi e reportistica dei record di audit | Analisi integrata dei record di audit	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-6(5)	Revisione, analisi e reportistica dei record di audit | Analisi integrata dei record di audit	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-7(1)	Riduzione dei record di audit e generazione di report | Elaborazione automatica	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
AU-9(2)	Protezione delle informazioni di audit | Archiviazione su sistemi o componenti fisici separati	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9(2)	Protezione delle informazioni di audit | Archiviazione su sistemi o componenti fisici separati	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9(2)	Protezione delle informazioni di audit | Archiviazione su sistemi o componenti fisici separati	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9(7)	Protezione delle informazioni di audit | Archiviazione su un componente con sistema operativo diverso	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU-9	Protezione delle informazioni di audit	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9	Protezione delle informazioni di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
AU-9	Protezione delle informazioni di audit	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9	Protezione delle informazioni di audit	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-9	Protezione delle informazioni di audit	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
AU-10	Non ripudio	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-10	Non ripudio	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-10	Non ripudio	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-10	Non ripudio	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-10	Non ripudio	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AU-10	Non ripudio	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-10	Non ripudio	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU-10	Non ripudio	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-10	Non ripudio	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU-10	Non ripudio	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-10	Non ripudio	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-10	Non ripudio	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	Generazione di record di audit	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	Generazione di record di audit	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	Generazione di record di audit	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	Generazione di record di audit	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
AU-12	Generazione di record di audit	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	Generazione di record di audit	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
AU-12	Generazione di record di audit	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	Generazione di record di audit	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
AU-12	Generazione di record di audit	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	Generazione di record di audit	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	Generazione di record di audit	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	Generazione di record di audit	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-12	Generazione di record di audit	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
AU-14(1)	Audit della sessione | Avvio del sistema	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registran do le azioni della Console di gestione e le chiamate API. AWS È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
CA-7	Monitoraggio continuo	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
CA-7	Monitoraggio continuo	s3-event-notifications-enabled	Le notifiche degli eventi di Amazon S3 possono notificar e al personale competente eventuali modifiche accidenta li o intenzionali agli oggetti del bucket. Gli avvisi includono: creazione di un nuovo oggetto, rimozione di oggetti, ripristino di oggetti, oggetti persi e replicati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
CA-7	Monitoraggio continuo	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
CA-7	Monitoraggio continuo	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CA-7	Monitoraggio continuo	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-7	Monitoraggio continuo	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi artefatti. AWS CodeBuild
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	rds-instance-default-admin-check	Poiché i nomi utente predefiniti sono di dominio pubblico, la loro modifica può aiutare a ridurre la superficie di attacco per le istanze database Amazon Relational Database Service (Amazon RDS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sat: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	redshift-default-admin-check	Poiché i nomi utente predefiniti sono di dominio pubblico, la loro modifica può aiutare a ridurre la superficie di attacco dei cluster Amazon Redshift.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CA-9(1)	Connessioni interne al sistema | Controlli di conformità	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2(2)	Configurazione di base | Supporto dell'automazione per accuratezza e aggiornamento	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2(2)	Configurazione di base | Supporto dell'automazione per accuratezza e aggiornamento	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2(2)	Configurazione di base | Supporto dell'automazione per accuratezza e aggiornamento	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2(2)	Configurazione di base | Supporto dell'automazione per accuratezza e aggiornamento	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2(2)	Configurazione di base | Supporto dell'automazione per accuratezza e aggiornamento	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2(2)	Configurazione di base | Supporto dell'automazione per accuratezza e aggiornamento	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	Configurazione di base	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
CM-2	Configurazione di base	rds-instance-default-admin-check	Poiché i nomi utente predefiniti sono di dominio pubblico, la loro modifica può aiutare a ridurre la superficie di attacco per le istanze database Amazon Relational Database Service (Amazon RDS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	Configurazione di base	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	Configurazione di base	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	Configurazione di base	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	Configurazione di base	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	Configurazione di base	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	Configurazione di base	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sat: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	Configurazione di base	redshift-default-admin-check	Poiché i nomi utente predefiniti sono di dominio pubblico, la loro modifica può aiutare a ridurre la superficie di attacco dei cluster Amazon Redshift.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-2	Configurazione di base	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
CM-3(6)	Controllo delle modifiche alla configurazione | Gestione della crittografia	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-3	Controllo delle modifiche alla configurazione	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-3	Controllo delle modifiche alla configurazione	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-7	Funzionalità minima	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
CM-7	Funzionalità minima	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-7	Funzionalità minima	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(1)	Inventario dei componenti di sistema | Aggiornamenti durante l'installazione e la rimozione	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(1)	Inventario dei componenti di sistema | Aggiornamenti durante l'installazione e la rimozione	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(2)	Inventario dei componenti di sistema | Manutenzione automatizzata	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(3)	Inventario dei componenti di sistema | Rilevamento automatico dei componenti non autorizzati	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(3)	Inventario dei componenti di sistema | Rilevamento automatico dei componenti non autorizzati	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(3)	Inventario dei componenti di sistema | Rilevamento automatico dei componenti non autorizzati	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8(3)	Inventario dei componenti di sistema | Rilevamento automatico dei componenti non autorizzati	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8	Inventario dei componenti di sistema	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CM-8	Inventario dei componenti di sistema	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-2(2)	Piano di emergenza | Pianificazione della capacità	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-2(2)	Piano di emergenza | Pianificazione della capacità	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(1)	Sito di archiviazione alternativo | Separazione dal sito primario	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(1)	Sito di archiviazione alternativo | Separazione dal sito primario	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(1)	Sito di archiviazione alternativo | Separazione dal sito primario	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(1)	Sito di archiviazione alternativo | Separazione dal sito primario	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(1)	Sito di archiviazione alternativo | Separazione dal sito primario	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(1)	Sito di archiviazione alternativo | Separazione dal sito primario	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(1)	Sito di archiviazione alternativo | Separazione dal sito primario	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(1)	Sito di archiviazione alternativo | Separazione dal sito primario	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6(2)	Sito di archiviazione alternativo | Obiettivi di tempo di ripristino e punto di ripristino	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6	Sito di archiviazione alternativo	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6	Sito di archiviazione alternativo	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6	Sito di archiviazione alternativo	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6	Sito di archiviazione alternativo	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6	Sito di archiviazione alternativo	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6	Sito di archiviazione alternativo	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6	Sito di archiviazione alternativo	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-6	Sito di archiviazione alternativo	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	Backup del sistema	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	Backup del sistema	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	Backup del sistema	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	Backup del sistema	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	Backup del sistema	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	Backup del sistema	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
CP-9	Backup del sistema	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	Backup del sistema	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	Backup del sistema	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	Backup del sistema	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sat: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	Backup del sistema	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-9	Backup del sistema	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
CP-10	Ripristino e ricostituzione del sistema	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
CP-10	Ripristino e ricostituzione del sistema	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CP-10	Ripristino e ricostituzione del sistema	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(1)	Identificazione e autenticazione (utenti dell'organizzazione) | Autenticazione a più fattori su account con privilegi	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(1)	Identificazione e autenticazione (utenti dell'organizzazione) | Autenticazione a più fattori su account con privilegi	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(1)	Identificazione e autenticazione (utenti dell'organizzazione) | Autenticazione a più fattori su account con privilegi	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(1)	Identificazione e autenticazione (utenti dell'organizzazione) | Autenticazione a più fattori su account con privilegi	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(2)	Identificazione e autenticazione (utenti dell'organizzazione) | Autenticazione a più fattori su account senza privilegi	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(2)	Identificazione e autenticazione (utenti dell'organizzazione) | Autenticazione a più fattori su account senza privilegi	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(2)	Identificazione e autenticazione (utenti dell'organizzazione) | Autenticazione a più fattori su account senza privilegi	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(2)	Identificazione e autenticazione (utenti dell'organizzazione) | Autenticazione a più fattori su account senza privilegi	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(6)	Identificazione e autenticazione (utenti dell'organizzazione) | Accesso agli account: dispositivo separato	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(6)	Identificazione e autenticazione (utenti dell'organizzazione) | Accesso agli account: dispositivo separato	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(6)	Identificazione e autenticazione (utenti dell'organizzazione) | Accesso agli account: dispositivo separato	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(6)	Identificazione e autenticazione (utenti dell'organizzazione) | Accesso agli account: dispositivo separato	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(8)	Identificazione e autenticazione (utenti dell'organizzazione) | Accesso agli account: resistenza a replay	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(8)	Identificazione e autenticazione (utenti dell'organizzazione) | Accesso agli account: resistenza a replay	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(8)	Identificazione e autenticazione (utenti dell'organizzazione) | Accesso agli account: resistenza a replay	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-2(8)	Identificazione e autenticazione (utenti dell'organizzazione) | Accesso agli account: resistenza a replay	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
IA-5(1)	Gestione degli autenticatori | Autenticazione basata su password	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-5(1)	Gestione degli autenticatori | Autenticazione basata su password	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
IA-5(1)	Gestione degli autenticatori | Autenticazione basata su password	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-5(1)	Gestione degli autenticatori | Autenticazione basata su password	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
IA-5(1)	Gestione degli autenticatori | Autenticazione basata su password	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-5(1)	Gestione degli autenticatori | Autenticazione basata su password	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-5(1)	Gestione degli autenticatori | Autenticazione basata su password	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-5(1)	Gestione degli autenticatori | Autenticazione basata su password	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IA-5(7)	Gestione degli autenticatori | Nessun autenticatore statico non crittografato incorporato	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-4(1)	Gestione degli incidenti | Processi di gestione degli incidenti automatizzati	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
IR-4(5)	Gestione degli incidenti | Disattivazione automatica del sistema	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RA-3(4)	Valutazione del rischio | Analisi informatica predittiva	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-3	Ciclo di vita di sviluppo del sistema	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-3	Ciclo di vita di sviluppo del sistema	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-8(19)	Principi di progettazione della sicurezza e della privacy | Protezione continua	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-8(21)	Principi di progettazione della sicurezza e della privacy | Autoanalisi	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-8(22)	Principi di progettazione della sicurezza e della privacy | Responsabilità e tracciabilità	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-8(25)	Principi di progettazione della sicurezza e della privacy | Sicurezza economica	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-11(1)	Test e valutazione per sviluppatori | Analisi statica del codice	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-11(6)	Test e valutazione per sviluppatori | Esame della superficie di attacco	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-15(2)	Processo, standard e strumenti di sviluppo | Strumenti di monitoraggio della sicurezza e della privacy	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-15(2)	Processo, standard e strumenti di sviluppo | Strumenti di monitoraggio della sicurezza e della privacy	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-15(8)	Processo, standard e strumenti di sviluppo | Riutilizzo delle informazioni su minacce e vulnerabilità	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SA-15(8)	Processo, standard e strumenti di sviluppo | Riutilizzo delle informazioni su minacce e vulnerabilità	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(1)	D enial-of-service Protezione | Limita la capacità di attaccare altri sistemi	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	D enial-of-service Protezione | Capacità, larghezza di banda e ridondanza	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	D enial-of-service Protection | Capacità, larghezza di banda e ridondanza	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	D enial-of-service Protection | Capacità, larghezza di banda e ridondanza	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	D enial-of-service Protection | Capacità, larghezza di banda e ridondanza	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	enial-of-service Protezione D | Capacità, larghezza di banda e ridondanza	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	enial-of-service Protezione D | Capacità, larghezza di banda e ridondanza	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	D enial-of-service Protezione | Capacità, larghezza di banda e ridondanza	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazion i che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	enial-of-service Protezione D | Capacità, larghezza di banda e ridondanza	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	enial-of-service Protezione D | Capacità, larghezza di banda e ridondanza	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	D enial-of-service Protection | Capacità, larghezza di banda e ridondanza	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
SC-5(2)	D enial-of-service Protezione | Capacità, larghezza di banda e ridondanza	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	enial-of-service Protezione D | Capacità, larghezza di banda e ridondanza	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	D enial-of-service Protezione | Capacità, larghezza di banda e ridondanza	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	enial-of-service Protezione D | Capacità, larghezza di banda e ridondanza	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	enial-of-service Protezione D | Capacità, larghezza di banda e ridondanza	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sat: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	D enial-of-service Protezione | Capacità, larghezza di banda e ridondanza	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	enial-of-service Protezione D | Capacità, larghezza di banda e ridondanza	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(2)	enial-of-service Protezione D | Capacità, larghezza di banda e ridondanza	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5(3)	D enial-of-service Protection | Rilevamento e monitoraggio	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-5	D Protezione enial-of-service	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
SC-7(3)	Protezione dei confini | Punti di accesso	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(3)	Protezione dei confini | Punti di accesso	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(3)	Protezione dei confini | Punti di accesso	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-7(3)	Protezione dei confini | Punti di accesso	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC-7(3)	Protezione dei confini | Punti di accesso	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC-7(3)	Protezione dei confini | Punti di accesso	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(3)	Protezione dei confini | Punti di accesso	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(4)	Protezione dei confini | Servizi di telecomunicazione esterni	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(5)	Protezione dei confini | Rifiuto per impostazione predefinita e consenso in via eccezionale	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(5)	Protezione dei confini | Rifiuto per impostazione predefinita e consenso in via eccezionale	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(5)	Protezione dei confini | Rifiuto per impostazione predefinita e consenso in via eccezionale	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(5)	Protezione dei confini | Rifiuto per impostazione predefinita e consenso in via eccezionale	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
SC-7(9)	Protezione dei confini | Limitazione del traffico di comunicazioni minacciose in uscita	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
SC-7(10)	Protezione dei confini | Prevenzione dell'esfiltrazione	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(11)	Protezione dei confini | Limitazione del traffico di comunicazioni in entrata	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	acm-certificate-expiration-check	Garantite che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(16)	Protezione dei confini | Prevenzione del rilevamento dei componenti di sistema	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(20)	Protezione dei confini | Isolamento dinamico e segregazione	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7(21)	Protezione dei confini | Isolamento dei componenti di sistema	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
SC-7	Protezione dei confini	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7	Protezione dei confini	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
SC-7	Protezione dei confini	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
SC-7	Protezione dei confini	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
SC-7	Protezione dei confini	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
SC-7	Protezione dei confini	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-7	Protezione dei confini	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Riservatezza e integrità della trasmissione | Protezione crittografica	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Riservatezza e integrità della trasmissione | Protezione crittografica	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-8(1)	Riservatezza e integrità della trasmissione | Protezione crittografica	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Riservatezza e integrità della trasmissione | Protezione crittografica	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
SC-8(1)	Riservatezza e integrità della trasmissione | Protezione crittografica	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Riservatezza e integrità della trasmissione | Protezione crittografica	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8(1)	Riservatezza e integrità della trasmissione | Protezione crittografica	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Riservatezza e integrità della trasmissione | Protezione crittografica	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-8(1)	Riservatezza e integrità della trasmissione | Protezione crittografica	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(1)	Riservatezza e integrità della trasmissione | Protezione crittografica	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8(2)	Riservatezza e integrità della trasmissione | Gestione prima e dopo la trasmissione	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(2)	Riservatezza e integrità della trasmissione | Gestione prima e dopo la trasmissione	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8(2)	Riservatezza e integrità della trasmissione | Gestione prima e dopo la trasmissione	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(2)	Riservatezza e integrità della trasmissione | Gestione prima e dopo la trasmissione	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8(2)	Riservatezza e integrità della trasmissione | Gestione prima e dopo la trasmissione	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(2)	Riservatezza e integrità della trasmissione | Gestione prima e dopo la trasmissione	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
SC-8(2)	Riservatezza e integrità della trasmissione | Gestione prima e dopo la trasmissione	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(2)	Riservatezza e integrità della trasmissione | Gestione prima e dopo la trasmissione	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-8(2)	Riservatezza e integrità della trasmissione | Gestione prima e dopo la trasmissione	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8(2)	Riservatezza e integrità della trasmissione | Gestione prima e dopo la trasmissione	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8	Riservatezza e integrità della trasmissione	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8	Riservatezza e integrità della trasmissione	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-8	Riservatezza e integrità della trasmissione	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8	Riservatezza e integrità della trasmissione	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
SC-8	Riservatezza e integrità della trasmissione	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8	Riservatezza e integrità della trasmissione	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
SC-8	Riservatezza e integrità della trasmissione	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8	Riservatezza e integrità della trasmissione	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-8	Riservatezza e integrità della trasmissione	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-8	Riservatezza e integrità della trasmissione	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-12(2)	Creazione e gestione delle chiavi crittografiche | Chiavi simmetriche	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12(2)	Creazione e gestione delle chiavi crittografiche | Chiavi simmetriche	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che le chiavi master del cliente (CMK) necessarie non siano pianificate per l'eliminazione in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12(3)	Creazione e gestione delle chiavi crittografiche | Chiavi asimmetriche	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-12(3)	Creazione e gestione delle chiavi crittografiche | Chiavi asimmetriche	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12(3)	Creazione e gestione delle chiavi crittografiche | Chiavi asimmetriche	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
SC-12(3)	Creazione e gestione delle chiavi crittografiche | Chiavi asimmetriche	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12(3)	Creazione e gestione delle chiavi crittografiche | Chiavi asimmetriche	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
SC-12(3)	Creazione e gestione delle chiavi crittografiche | Chiavi asimmetriche	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12(3)	Creazione e gestione delle chiavi crittografiche | Chiavi asimmetriche	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-12	Creazione e gestione delle chiavi crittografiche	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-12	Creazione e gestione delle chiavi crittografiche	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che le chiavi master del cliente (CMK) necessarie non siano pianificate per l'eliminazione in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
SC-13	Protezione crittografica	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
SC-13	Protezione crittografica	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-13	Protezione crittografica	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.
SC-13	Protezione crittografica	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-13	Protezione crittografica	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
SC-13	Protezione crittografica	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
SC-13	Protezione crittografica	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
SC-13	Protezione crittografica	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
SC-13	Protezione crittografica	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
SC-13	Protezione crittografica	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-13	Protezione crittografica	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
SC-13	Protezione crittografica	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
SC-13	Protezione crittografica	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
SC-13	Protezione crittografica	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
SC-13	Protezione crittografica	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-13	Protezione crittografica	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
SC-13	Protezione crittografica	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23(3)	Autenticità della sessione | Identificatori di sessione univoci generati dal sistema	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-23(3)	Autenticità della sessione | Identificatori di sessione univoci generati dal sistema	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23(3)	Autenticità della sessione | Identificatori di sessione univoci generati dal sistema	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
SC-23(3)	Autenticità della sessione | Identificatori di sessione univoci generati dal sistema	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23(3)	Autenticità della sessione | Identific atori di sessione univoci generati dal sistema	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
SC-23(3)	Autenticità della sessione | Identific atori di sessione univoci generati dal sistema	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23(3)	Autenticità della sessione | Identificatori di sessione univoci generati dal sistema	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-23(3)	Autenticità della sessione | Identificatori di sessione univoci generati dal sistema	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23(3)	Autenticità della sessione | Identificatori di sessione univoci generati dal sistema	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-23(5)	Autenticità della sessione | Autorità di certificazione consentite	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23(5)	Autenticità della sessione | Autorità di certificazione consentite	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23	Autenticità della sessione	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-23	Autenticità della sessione	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23	Autenticità della sessione	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
SC-23	Autenticità della sessione	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23	Autenticità della sessione	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
SC-23	Autenticità della sessione	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23	Autenticità della sessione	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SC-23	Autenticità della sessione	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-23	Autenticità della sessione	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-23	Autenticità della sessione	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi artefatti. AWS CodeBuild

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
SC-28(1)	Protezione delle informazioni a riposo | Protezione crittografica	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28(3)	Protezione delle informazioni a riposo | Chiavi crittografiche	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
SC-28(3)	Protezione delle informazioni a riposo | Chiavi crittografiche	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che vengano ruotate dopo aver raggiunto la fine del periodo crittografico.
SC-28	Protezione delle informazioni a riposo	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Protezione delle informazioni a riposo	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
SC-28	Protezione delle informazioni a riposo	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Protezione delle informazioni a riposo	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.
SC-28	Protezione delle informazioni a riposo	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
SC-28	Protezione delle informazioni a riposo	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Protezione delle informazioni a riposo	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Protezione delle informazioni a riposo	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
SC-28	Protezione delle informazioni a riposo	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Protezione delle informazioni a riposo	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
SC-28	Protezione delle informazioni a riposo	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
SC-28	Protezione delle informazioni a riposo	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Protezione delle informazioni a riposo	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
SC-28	Protezione delle informazioni a riposo	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
SC-28	Protezione delle informazioni a riposo	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Protezione delle informazioni a riposo	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Protezione delle informazioni a riposo	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
SC-28	Protezione delle informazioni a riposo	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-28	Protezione delle informazioni a riposo	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
SC-28	Protezione delle informazioni a riposo	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-36(2)	Elaborazione e archiviazione distribuite | Sincronizzazione	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-36	Elaborazione e archiviazione distribuite	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-36	Elaborazione e archiviazione distribuite	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SC-36	Elaborazione e archiviazione distribui te	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
SC-36	Elaborazione e archiviazione distribuite	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(2)	Correzione dei difetti | Stato della correzione automatizzata dei difetti	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(2)	Correzione dei difetti | Stato della correzione automatizzata dei difetti	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(2)	Correzione dei difetti | Stato della correzione automatizzata dei difetti	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sat: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(3)	Correzione dei difetti | Tempo di correzione dei difetti e benchmark per le azioni correttive	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(3)	Correzione dei difetti | Tempo di correzione dei difetti e benchmark per le azioni correttive	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(3)	Correzione dei difetti | Tempo di correzione dei difetti e benchmark per le azioni correttive	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
SI-2(4)	Correzione dei difetti | Strumenti automatici di gestione delle patch	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(4)	Correzione dei difetti | Strumenti automatici di gestione delle patch	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(4)	Correzione dei difetti | Strumenti automatici di gestione delle patch	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sat: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(5)	Correzione dei difetti | Aggiornamenti automatici di software e firmware	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(5)	Correzione dei difetti | Aggiornamenti automatici di software e firmware	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2(5)	Correzione dei difetti | Aggiornamenti automatici di software e firmware	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sat: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2	Correzione dei difetti	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2	Correzione dei difetti	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2	Correzione dei difetti	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2	Correzione dei difetti	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2	Correzione dei difetti	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2	Correzione dei difetti	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
SI-2	Correzione dei difetti	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2	Correzione dei difetti	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-2	Correzione dei difetti	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sat: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3(8)	Protezione da codice dannoso | Rilevamento di comandi non autorizzati	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3(8)	Protezione da codice dannoso | Rilevamento di comandi non autorizzati	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3(8)	Protezione da codice dannoso | Rilevamento di comandi non autorizzati	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
SI-3(8)	Protezione da codice dannoso | Rilevamento di comandi non autorizzati	s3-event-notifications-enabled	Le notifiche degli eventi di Amazon S3 possono notificare e al personale competente eventuali modifiche accidentali o intenzionali agli oggetti del bucket. Gli avvisi includono: creazione di un nuovo oggetto, rimozione di oggetti, ripristino di oggetti, oggetti persi e replicati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3(8)	Protezione da codice dannoso | Rilevamento di comandi non autorizzati	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
SI-3(8)	Protezione da codice dannoso | Rilevamento di comandi non autorizzati	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3(8)	Protezione da codice dannoso | Rilevamento di comandi non autorizzati	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
SI-3(8)	Protezione da codice dannoso | Rilevamento di comandi non autorizzati	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3(8)	Protezione da codice dannoso | Rilevamento di comandi non autorizzati	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3(8)	Protezione da codice dannoso | Rilevamento di comandi non autorizzati	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-3(8)	Protezione da codice dannoso | Rilevamento di comandi non autorizzati	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(1)	Monitoraggio del sistema | Sistema di rilevamento delle intrusioni a livello di sistema	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(2)	Monitoraggio del sistema | Strumenti e meccanismi automatizzati per l'analisi in tempo reale	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
SI-4(4)	Monitoraggio del sistema | Traffico di comunicazioni in entrata e in uscita	s3-event-notifications-enabled	Le notifiche degli eventi di Amazon S3 possono notificare al personale competente eventuali modifiche accidentali o intenzionali agli oggetti del bucket. Gli avvisi includono: creazione di un nuovo oggetto, rimozione di oggetti, ripristino di oggetti, oggetti persi e replicati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(4)	Monitoraggio del sistema | Traffico di comunicazioni in entrata e in uscita	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(5)	Monitoraggio del sistema | Avvisi generati dal sistema	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(5)	Monitoraggio del sistema | Avvisi generati dal sistema	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
SI-4(5)	Monitoraggio del sistema | Avvisi generati dal sistema	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(12)	Monitoraggio del sistema | Avvisi automatici generati dall'organizzazione	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(13)	Monitoraggio del sistema | Analisi dei modelli di traffico ed eventi	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(20)	Monitoraggio del sistema | Utenti con privilegi	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(20)	Monitoraggio del sistema | Utenti con privilegi	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(20)	Monitoraggio del sistema | Utenti con privilegi	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
SI-4(20)	Monitoraggio del sistema | Utenti con privilegi	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(20)	Monitoraggio del sistema | Utenti con privilegi	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
SI-4(20)	Monitoraggio del sistema | Utenti con privilegi	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(20)	Monitoraggio del sistema | Utenti con privilegi	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(20)	Monitoraggio del sistema | Utenti con privilegi	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(20)	Monitoraggio del sistema | Utenti con privilegi	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(22)	Monitoraggio del sistema | Servizi di rete non autorizzati	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4(25)	Monitoraggio del sistema | Ottimizzazione dell'analisi del traffico di rete	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
SI-4	Monitoraggio del sistema	s3-event-notifications-enabled	Le notifiche degli eventi di Amazon S3 possono notificare e al personale competente eventuali modifiche accidentali o intenzionali agli oggetti del bucket. Gli avvisi includono: creazione di un nuovo oggetto, rimozione di oggetti, ripristino di oggetti, oggetti persi e replicati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	Monitoraggio del sistema	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-4	Monitoraggio del sistema	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(1)	Integrità di software, firmware e informazioni | Controlli di integrità	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(3)	Integrità di software, firmware e informazioni | Strumenti per l'integrità gestiti a livello centralizzato	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi artefatti. AWS CodeBuild

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(6)	Integrità di software, firmware e informazioni | Protezione crittografica	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(7)	Integrità di software, firmware e informazioni | Integrazione di rilevamento e risposta	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-7(8)	Integrità di software, firmware e informazioni | Capacità di audit per eventi significativi	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	Gestione e conservazione delle informazioni	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	Gestione e conservazione delle informazioni	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	Gestione e conservazione delle informazioni	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	Gestione e conservazione delle informazioni	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	Gestione e conservazione delle informazioni	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	Gestione e conservazione delle informazioni	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-12	Gestione e conservazione delle informazioni	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	s3-version-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-13(5)	Prevenzione di guasti prevedibili | Capacità di failover	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-20	Taint	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
SI-20	Taint	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
SI-20	Taint	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NIST 800-53 rev 5.

Best practice operative per NIST 800 171

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il NIST 800-171 e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli NIST 800-171. Un controllo NIST 800 171 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearc h

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizza ti (compresi altri sistemi).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.1	Limita l'accesso al sistema agli utenti, ai processi che agiscono per loro conto o ai dispositivi autorizzati (compresi altri sistemi).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizza ti possono eseguire.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizza ti possono eseguire.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.2	Limita l'accesso al sistema ai tipi di transazioni e funzioni che gli utenti autorizzati possono eseguire.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearc h

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearc h Service all'inter no di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Information) conformemente alle autorizzazioni approvate.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3	Controllo del flusso di CUI (Controlled Unclassified Informati on) conformemente alle autorizzazioni approvate.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearc h

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.4	Separazione dei compiti dei singoli per ridurre il rischio di attività dannose senza collusione.	s3-bucket-policy-grantee-check	Gestisci l'accesso al cloud abilitando s3_ bucket_policy_grantee_check . AWS Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ecs-containers-non privileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.5	Utilizzo del principio del privilegio minimo, anche per funzioni di sicurezza specifiche e account privilegiati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al cloud abilitando s3_ bucket_policy_grantee_check . AWS Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.6	Utilizzo di account o ruoli senza privilegi per accedere a funzioni non di sicurezza.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
3.1.7	Impedisci agli utenti senza privilegi di eseguire funzioni con privilegi ed effettua l'audit dell'esecuzione di tali funzioni.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.7	Impedisci agli utenti senza privilegi di eseguire funzioni con privilegi ed effettua l'audit dell'esecuzione di tali funzioni.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
3.1.7	Impedisci agli utenti senza privilegi di eseguire funzioni con privilegi ed effettua l'audit dell'esecuzione di tali funzioni.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.7	Impedisci agli utenti senza privilegi di eseguire funzioni con privilegi ed effettua l'audit dell'esecuzione di tali funzioni.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.7	Impedisci agli utenti senza privilegi di eseguire funzioni con privilegi ed effettua l'audit dell'esecuzione di tali funzioni.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.7	Impedisci agli utenti senza privilegi di eseguire funzioni con privilegi ed effettua l'audit dell'esecuzione di tali funzioni.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
3.1.7	Impedisci agli utenti senza privilegi di eseguire funzioni con privilegi ed effettua l'audit dell'esecuzione di tali funzioni.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,1,12	Monitoraggio e controllo delle sessioni di accesso remoto.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,1,12	Monitoraggio e controllo delle sessioni di accesso remoto.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,1,12	Monitoraggio e controllo delle sessioni di accesso remoto.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.12	Monitoraggio e controllo delle sessioni di accesso remoto.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,1,12	Monitoraggio e controllo delle sessioni di accesso remoto.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
3,1,13	Utilizzo di meccanism i crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3,1,13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,1,13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
3,1,13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
3.1.13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,1,13	Utilizzo di meccanismi crittografici per la protezione della riservatezza delle sessioni di accesso remoto.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3,1,14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,1,14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
3,1,14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.14	Indirizza l'accesso remoto tramite punti di controllo degli accessi gestiti.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.20	Verifica e controlla /limita le connessioni e l'uso di sistemi esterni.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
31,20	Verifica e controlla /limita le connessioni e l'uso di sistemi esterni.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.20	Verifica e controlla /limita le connessioni e l'uso di sistemi esterni.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.20	Verifica e controlla /limita le connessioni e l'uso di sistemi esterni.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.20	Verifica e controlla /limita le connessioni e l'uso di sistemi esterni.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.20	Verifica e controlla /limita le connessioni e l'uso di sistemi esterni.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.20	Verifica e controlla /limita le connessioni e l'uso di sistemi esterni.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.20	Verifica e controlla /limita le connessioni e l'uso di sistemi esterni.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
3.1.20	Verifica e controlla /limita le connessioni e l'uso di sistemi esterni.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.20	Verifica e controlla /limita le connessio ni e l'uso di sistemi esterni.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.20	Verifica e controlla /limita le connessioni e l'uso di sistemi esterni.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	cw-loggroup-retent ion-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzio ne dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruz ione e l'identificazione di eventi potenzial mente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearc h di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservaz ione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibi lità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizzate o inappropriate.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessaria per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizzate o inappropriate.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
3.3.1	Crea e conserva record di audit del sistema nella misura necessaria per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizzate o inappropriate.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicaz ione centrale all'inter no di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettaglia te sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearc h di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearc h I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosti care problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.1	Crea e conserva record di audit del sistema nella misura necessari a per consentire il monitoraggio, l'analisi, l'indagine e la segnalazione di attività di sistema illegali, non autorizza te o inappropriate.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.2	Garanzia che le azioni dei singoli utenti del sistema possano essere ricondotte in modo univoco a tali utenti affinché questi possano essere ritenuti responsabili delle loro azioni.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.4	Avvisa in caso di errore del processo di audit.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.4	Avvisa in caso di errore del processo di audit.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.5	Metti in correlazione i processi di revisione, analisi e reporting di audit per le indagini e la risposta alle indicazioni di attività inappropriate, sospette o insolite.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.5	Metti in correlazione i processi di revisione, analisi e reporting di audit per le indagini e la risposta alle indicazioni di attività inappropriate, sospette o insolite.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
3.3.8	Proteggi le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.8	Proteggi le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.8	Proteggi le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.8	Proteggi le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.8	Proteggi le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS Cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
3.3.8	Proteggi le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.8	Proteggi le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.3.8	Proteggi le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3.8	Proteggi le informazioni e gli strumenti di audit da accessi, modifiche ed eliminazioni non autorizzati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.1	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-security-group-attached-to-eni-periodic	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.1	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.1	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.1	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.1	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.1	Individuazione e mantenimento delle configurazioni di base e degli inventari dei sistemi dell'organizzazione (compresi hardware, software, firmware e documentazione) durante i rispettivi cicli di vita del sistema.	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurando che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.6	Utilizzo del principio della minima funzionalità configurando i sistemi dell'organizzazione in modo da fornire solo le funzionalità essenziali.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.4.7	Limita, disabilita e previeni l'utilizzo di funzioni, porte, protocolli o servizi non essenziali.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.7	Limita, disabilita e previeni l'utilizzo di funzioni, porte, protocolli o servizi non essenziali.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.7	Limita, disabilita e previeni l'utilizzo di funzioni, porte, protocolli o servizi non essenziali.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.7	Limita, disabilita e previeni l'utilizzo di funzioni, porte, protocolli o servizi non essenziali.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.9	Controllo e monitoraggio del software installato dall'utente.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.9	Controllo e monitoraggio del software installato dall'utente.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.2	Autentica (o verifica) le identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi dell'organizzazione.	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.2	Autentica (o verifica) le identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi dell'orga nizzazione.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.2	Autentica (o verifica) le identità di tali utenti, processi o dispositivi, come prerequisito per consentire l'accesso ai sistemi dell'orga nizzazione.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.3	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.3	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.3	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.3	Utilizzo dell'autenticazione a più fattori per l'accesso locale e di rete agli account con privilegi e per l'accesso di rete agli account senza privilegi.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.5	Impedisci il riutilizzo degli identificatori per un determinato periodo.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.6	Disattivazione degli identificatori dopo un determinato periodo di inattività.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.7	Applicazione di una complessità minima della password e cambio di caratteri quando vengono create nuove password.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.8	Divieto di riutilizzo della password per un determinato numero di generazioni.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.10	Archiviazione e trasmissione di sole password protette da crittografia.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.1	Impostazione di una capacità operativa di gestione degli incidenti per i sistemi dell'organizzazione che includa attività di preparazione, rilevamento, analisi, contenimento, ripristino e risposta agli utenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.11.2	Scansiona le vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione a intervalli regolari e quando vengono identificate nuove vulnerabilità che interessano il sistema.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.11.2	Scansiona le vulnerabilità nei sistemi e nelle applicazioni dell'organizzazione a intervalli regolari e quando vengono identificate nuove vulnerabilità che interessano il sistema.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.11.3	Correggi le vulnerabilità in base alle valutazioni del rischio.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
3,13,1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
3,13,1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3,13,1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,1	Monitora, controlla e proteggi le comunicazioni (ovvero le informazioni trasmesse o ricevute dai sistemi dell'organizzazione) sui perimetri esterni e sui perimetri interni chiave dei sistemi dell'organizzazione.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
3,13,2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	codebuild-project-source-repo-url-check	Assicurati che l' GitHub URL del repository di origine di Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
3,13,2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
3,13,2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearc h

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
3,13,2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.2	Utilizzo di progetti architetturali, tecniche di sviluppo del software e principi di ingegneria dei sistemi che promuovono un'efficace sicurezza delle informazioni all'interno dei sistemi dell'organizzazione.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.6	Nega il traffico delle comunicazioni di rete per impostazi one predefinita e consenti il traffico delle comunicazioni di rete per eccezione (ovvero, negare tutto, consentire per eccezione).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.6	Nega il traffico delle comunicazioni di rete per impostazi one predefinita e consenti il traffico delle comunicazioni di rete per eccezione (ovvero, negare tutto, consentire per eccezione).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.6	Nega il traffico delle comunicazioni di rete per impostazione predefinita e consenti il traffico delle comunicazioni di rete per eccezione (ovvero, negare tutto, consentire per eccezione).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
3,13,8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3,13,8	Implementazione di meccanismi crittografici per prevenire la divulgazione non autorizzata di CUI (Controlled Unclassified Information) durante la trasmissione, a meno che non siano altrimenti protette da misure di protezione fisiche alternative.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,10	Definizione e gestione delle chiavi crittografiche per la crittografia impiegata nei sistemi organizzativi.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.
3.13.10	Definizione e gestione delle chiavi crittografiche per la crittografia impiegata nei sistemi organizzativi.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
3,13,16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo notebook. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassif ied Information) a riposo.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassif ied Information) a riposo.	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,13,16	Protezione della riservatezza delle CUI (Controlled Unclassified Information) a riposo.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.16	Protezione della riservatezza delle CUI (Controlled Unclassif ied Information) a riposo.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.
3,13,16	Protezione della riservatezza delle CUI (Controlled Unclassif ied Information) a riposo.	sagemaker-endpoint -configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.1	Identifica, segnala e correggi in modo tempestivo i difetti delle informazioni e del sistema.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.1	Identifica, segnala e correggi in modo tempestivo i difetti delle informazioni e del sistema.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.2	Fornisci protezione da codice dannoso in posizioni appropriate all'interno dei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.2	Fornisci protezione da codice dannoso in posizioni appropriate all'interno dei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.3	Monitora gli avvisi e i suggerimenti di sicurezza del sistema e intervieni in risposta.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.3	Monitora gli avvisi e i suggerimenti di sicurezza del sistema e intervieni in risposta.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.3	Monitora gli avvisi e i suggerimenti di sicurezza del sistema e intervieni in risposta.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,14,3	Monitora gli avvisi e i suggerimenti di sicurezza del sistema e intervieni in risposta.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.3	Monitora gli avvisi e i suggerimenti di sicurezza del sistema e intervieni in risposta.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.4	Aggiorna i meccanismi di protezione da codice dannoso quando sono disponibili nuove versioni.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,14,6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.6	Monitoraggio dei sistemi dell'organizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
3.14.6	Monitoraggio dei sistemi dell'organizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,14,6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicaz ione centrale all'inter no di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettaglia te sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,14,6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.6	Monitoraggio dei sistemi dell'organizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,14,6	Monitoraggio dei sistemi dell'orga nizzazione, compreso il traffico delle comunicazioni in entrata e in uscita, per rilevare attacchi e indicatori di potenziali attacchi.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,144,7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,144,7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,144,7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,144,7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3,144,7	Individuazione dell'uso non autorizzato dei sistemi dell'organizzazione.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NIST 800 171.

Best practice operative per NIST 800 172

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il NIST 800-172 e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli NIST 800-172. Un controllo NIST 800-172 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	domini di sicurezza sui sistemi connessi.		provenienza delle richieste dal Gateway API.
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	alb-desync-mode-check	Per contribuire a proteggere le applicazioni dalle vulnerabilità della desincronizzazione HTTP, assicurati che la modalità di mitigazione della desincronizzazione HTTP sia abilitata sui sistemi di bilanciamento del carico delle applicazioni. I problemi di desincronizzazione HTTP possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della cache e della coda delle richieste. Le modalità di mitigazione della desincronizzazione sono Monitoraggio, Difensiva e Più rigorosa. Difensiva è la modalità predefinita.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	clb-desync-mode-check	Per contribuire a proteggere le applicazioni dalle vulnerabilità della desincronizzazione HTTP, assicurati che la modalità di mitigazione della desincronizzazione HTTP sia abilitata sui sistemi di bilanciamento del carico delle applicazioni. I problemi di desincronizzazione HTTP possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della cache e della coda delle richieste. Le modalità di mitigazione della desincronizzazione sono Monitoraggio, Difensiva e Più rigorosa. Difensiva è la modalità predefinita.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	ec2-token-hop-limit-check	Assicurati che la risposta HTTP PUT del servizio di metadati di istanza (IMDS) sia limitata all'istanza Amazon Elastic Compute Cloud (Amazon EC2). Con IMDSv2, la risposta PUT che contiene il token segreto per impostazione predefinita non può uscire dall'istanza, poiché il limite di hop di risposta dei metadati è impostato su 1 (valore di configurazione predefinito). Se questo valore è maggiore di 1, il token può lasciare l'istanza EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1.3e	Impiega [Assegnazione: soluzioni di trasferimento sicuro delle informazioni definite dall'organizzazione] per controllare i flussi di informazioni tra i domini di sicurezza sui sistemi connessi.	nacl-no-unrestricted-ssh-rdp	Le porte di amministrazione del server remoto nelle liste di controllo degli accessi alla rete (ACL), come la porta 22 (SSH) e la porta 3389 (RDP), non devono essere accessibili pubblicamente, in quanto ciò potrebbe comportare l'accesso indesiderato alle risorse nel VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.2.1e	Offri una formazione di sensibilizzazione [Assegnazione: frequenza definita dall'organizzazione] incentrata sul riconoscimento, e sulla relativa risposta, delle minacce provenienti da ingegneria sociale, autori di minacce persistenti avanzate, violazioni e comportamenti sospetti; aggiorna la formazione [Assegnazione: frequenza definita dall'organizzazione] o in caso di cambiamenti significativi della minaccia.	security-awareness-program-exists (controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.2e	Utilizza meccanismi automatizzati per rilevare componenti di sistema mal configurati o non autorizzati; dopo il rilevamento, [Selezione (una o più): rimuovi i componenti; colloca i componenti in una rete di quarantena o di correzione] per facilitare l'applicazione di patch, la riconfigurazione o altre misure di mitigazione.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.2e	Utilizza meccanismi automatizzati per rilevare componenti di sistema mal configurati o non autorizzati; dopo il rilevamento, [Selezione (una o più): rimuovi i componenti; colloca i componenti in una rete di quarantena o di correzione] per facilitare l'applicazione di patch, la riconfigurazione o altre misure di mitigazione.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.2e	Utilizza meccanismi automatizzati per rilevare componenti di sistema mal configurati o non autorizzati; dopo il rilevamento, [Selezione (una o più): rimuovi i componenti; colloca i componenti in una rete di quarantena o di correzione] per facilitare l'applicazione di patch, la riconfigurazione o altre misure di mitigazione.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.2e	Utilizza meccanismi automatizzati per rilevare componenti di sistema mal configurati o non autorizzati; dopo il rilevamento, [Selezione (una o più): rimuovi i componenti; colloca i componenti in una rete di quarantena o di correzione] per facilitare l'applicazione di patch, la riconfigurazione o altre misure di mitigazione.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.3e	Utilizza strumenti di rilevamento e gestione automatizzati per mantenere un inventario completo up-to-date, accurato e immediatamente disponibile dei componenti del sistema.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.3e	Utilizza strumenti di rilevamento e gestione automatiz zati per mantenere un inventario completo up-to-date, accurato e immediatamente disponibile dei componenti del sistema.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.3e	Utilizza strumenti di rilevamento e gestione automatizzati per mantenere un inventario completo up-to-date, accurato e immediatamente disponibile dei componenti del sistema.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4.3e	Utilizza strumenti di rilevamento e gestione automatizzati per mantenere un inventario completo up-to-date, accurato e immediatamente disponibile dei componenti del sistema.	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
3.4.3e	Utilizza strumenti di rilevamento e gestione automatizzati per mantenere un inventario completo up-to-date, accurato e immediatamente disponibile dei componenti del sistema.	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.2e	Utilizza meccanismi automatizzati per la generazione, la protezione, la rotazione e la gestione delle password per sistemi e componenti di sistema che non supportano l'autenticazione a più fattori o una gestione complessa degli account.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.2e	Utilizza meccanismi automatizzati per la generazione, la protezione, la rotazione e la gestione delle password per sistemi e componenti di sistema che non supportano l'autenticazione a più fattori o una gestione complessa degli account.	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.
3.5.2e	Utilizza meccanismi automatizzati per la generazione, la protezione, la rotazione e la gestione delle password per sistemi e componenti di sistema che non supportano l'autenticazione a più fattori o una gestione complessa degli account.	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.2e	Utilizza meccanismi automatizzati per la generazione, la protezione e, la rotazione e la gestione delle password per sistemi e componenti di sistema che non supportano l'autenticazione a più fattori o una gestione complessa degli account.	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.11.1e	Utilizza [Assegnazione: fonti di intelligence sulle minacce definite dall'organizzazione] nell'ambito di una valutazione del rischio per guidare e orientare lo sviluppo dei sistemi dell'organizzazione, le architetture di sicurezza, la scelta delle soluzioni di sicurezza, il monitoraggio, la ricerca delle minacce e le attività di risposta e ripristino.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.11.2e	Conduci attività di ricerca delle minacce informati che [Selezione (una o più): [Assegnazione: frequenza definita dall'organizzazion e]; [Assegnazione: evento definito dall'organizzazione]] per cercare indicator i di compromis sione in [Assegnaz ione: sistemi definiti dall'organizzazione] e rilevare, tracciare e fermare le minacce che eludono i controlli esistenti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
3.11.5e	Valuta l'efficacia delle soluzioni di sicurezza [Assegnazione: frequenza definita dall'organizzazione] per affrontare i rischi previsti per i sistemi dell'organizzazione e l'organizzazione stessa in base all'intel ligence sulle minacce attuale e accumulata.	annual-risk-assess ment-performed (controllo del processo)	Esegui una valutazio ne annuale del rischio sulla tua organizza zione. Le valutazioni del rischio possono aiutare a determina re la probabilità e l'impatto dei rischi e/o delle vulnerabi lità identificati che interessano un'organi zzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	nacl-no-unrestricted-ssh-rdp	Le porte di amministrazione del server remoto nelle liste di controllo degli accessi alla rete (ACL), come la porta 22 (SSH) e la porta 3389 (RDP), non devono essere accessibili pubblicamente, in quanto ciò potrebbe comportare l'accesso indesiderato alle risorse nel VPC.
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.13.4e	Utilizza [Selezione: (una o più): [Assegnazione: tecniche di isolamento fisico definite dall'organizzazione]; [Assegnazione: tecniche di isolamento logico definite dall'organizzazione]] nei sistemi dell'organizzazione e nei componenti di sistema.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.1e	Verifica l'integrità di [Assegnazione: software essenziale o critico per la sicurezza definito dall'orga nizzazione] utilizzan do meccanismi con radice di attendibilità o firme crittografiche.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integri tà dei log. CloudTrai l La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificar e, eliminare o falsifica re i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.2e	Monitora continuamente i sistemi dell'organizzazione e i componenti di sistema per rilevare comportamenti anomali o sospetti.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
3.14.2e	Monitora continuamente i sistemi dell'organizzazione e i componenti di sistema per rilevare comportamenti anomali o sospetti.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.2e	Monitora continuamente i sistemi dell'organizzazione e i componenti di sistema per rilevare comportamenti anomali o sospetti.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.2e	Monitora continuamente i sistemi dell'organizzazione e i componenti di sistema per rilevare comportamenti anomali o sospetti.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.2e	Monitora continuamente i sistemi dell'organizzazione e i componenti di sistema per rilevare comportamenti anomali o sospetti.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.2e	Monitora continuamente i sistemi dell'organizzazione e i componenti di sistema per rilevare comportamenti anomali o sospetti.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.2e	Monitora continuamente i sistemi dell'organizzazione e i componenti di sistema per rilevare comportamenti anomali o sospetti.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.6e	Utilizza informazioni sugli indicatori di minaccia e mitigazioni efficaci ottenute da [Assegnazione: organizzazioni esterne definite dall'organizzazione] per guidare e orientare il rilevamento delle intrusioni e la ricerca delle minacce.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.7e	Verifica la correttezza di [Assegnazione: componenti software, firmware e hardware essenziali o critici per la sicurezza definiti dall'organizzazione] utilizzando [Assegnazione: metodi o tecniche di verifica definiti dall'organizzazione].	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.7e	Verifica la correttezza di [Assegnazione: componenti software, firmware e hardware essenziali o critici per la sicurezza definiti dall'organizzazione] utilizzando [Assegnazione: metodi o tecniche di verifica definiti dall'organizzazione].	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.7e	Verifica la correttezza di [Assegnazione: componenti software, firmware e hardware essenziali o critici per la sicurezza definiti dall'organizzazione] utilizzando [Assegnazione: metodi o tecniche di verifica definiti dall'organizzazione].	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.7e	Verifica la correttezza di [Assegnazione: componenti software, firmware e hardware essenziali o critici per la sicurezza definiti dall'organizzazione] utilizzando [Assegnazione: metodi o tecniche di verifica definiti dall'organizzazione].	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribuiti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.14.7e	Verifica la correttezza di [Assegnazione: componenti software, firmware e hardware essenziali o critici per la sicurezza definiti dall'organizzazione] utilizzando [Assegnazione: metodi o tecniche di verifica definiti dall'organizzazione].	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilitazione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NIST 800 172.

Best practice operative per NIST 800 181

I pacchetti di conformità forniscono un framework di conformità generico progettato per consentire di creare controlli di governance della sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il NIST 800 181 e le regole AWS Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli NIST 800 181. Un controllo NIST 800 181 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	dynamodb-pitr-enab led	Abilita questa regola per verificare che sia stato eseguito il backup delle informazi oni. Inoltre, mantiene i backup assicuran do che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristin o mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
T0008	Analizza e pianifica le modifiche previste nei requisiti di capacità dei dati.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	acm-certificate-expiration-check	Garantisci la protezione e dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservate zza, integrità e disponibilità dell'orga nizzazione.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservate zza, integrità e disponibilità dell'orga nizzazione.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che le chiavi master dei clienti (CMK) necessarie non siano pianificate per l'eliminazione in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	opensearch-encrypted-at-rest	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i domini Amazon Elasticsearch Service (Amazon ES).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservate zza, integrità e disponibilità dell'orga nizzazione.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservate zza, integrità e disponibilità dell'orga nizzazione.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0017	Applica i principi dell'architettura di sicurezza orientata ai servizi per soddisfare i requisiti di riservatezza, integrità e disponibilità dell'organizzazione.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0024	Raccogli e mantieni i dati necessari per la creazione di report sulla cibersicurezza dei sistemi.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0042	Collabora con gli analisti della difesa informatica per gestire e amministrare l'aggiornamento di regole e firme (ad esempio, sistemi di rilevamento/protezione dalle intrusioni, antivirus e liste nere dei contenuti) per applicazioni specializzate di difesa informatica.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0047	Correla i dati sugli incidenti per identific are vulnerabilità specifiche e formulare raccomandazioni per una rapida risoluzio ne.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuità delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternativo, backup e supporto dei materiali per il ripristino del sistema.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
T0051	Definisci i livelli appropriati di disponibilità del sistema in base alle sue funzioni critiche e assicurati che i requisiti di sistema identifichino i giusti requisiti di ripristino di emergenza e continuit à delle operazioni, includendo qualsiasi requisito appropriato di failover/sito alternati vo, backup e supporto dei materiali per il ripristino del sistema.	ec2-resources-prot ected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
T0065	Sviluppa e implementa procedure di backup e ripristino di rete.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizza zione. In particola re, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVers ionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltati vamente il preferred MaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotR etention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0065	Sviluppa e implement a procedure di backup e ripristino di rete.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0070	Sviluppa piani di ripristino di emergenza e continuità delle operazioni per i sistemi in fase di sviluppo e assicura l'esecuzione dei test prima che i sistemi entrino in un ambiente di produzione.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0086	Assicurati che l'applicazione delle patch di sicurezza per i prodotti commercia li integrati nella progettazione del sistema rispetti le tempistiche dettate dall'autorità di gestione per l'ambient e operativo previsto.	rds-automatic-mino r-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'install azione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relaziona le (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0086	Assicurati che l'applicazione delle patch di sicurezza per i prodotti commercia li integrati nella progettazione del sistema rispetti le tempistiche dettate dall'autorità di gestione per l'ambient e operativo previsto.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0086	Assicurati che l'applicazione delle patch di sicurezza per i prodotti commercia li integrati nella progettazione del sistema rispetti le tempistiche dettate dall'autorità di gestione per l'ambient e operativo previsto.	elastic-beanstalk-managed-updates-en abled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0086	Assicurati che l'applicazione delle patch di sicurezza per i prodotti commercia li integrati nella progettazione del sistema rispetti le tempistiche dettate dall'autorità di gestione per l'ambient e operativo previsto.	redshift-cluster-m aintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizza zione. In particola re, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVers ionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltati vamente il preferred MaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotR etention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0110	Identifica e/o determina se un incidente di sicurezza è indicativo di una violazione della legge che richiede azioni legali specifiche.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0110	Identifica e/o determina se un incidente di sicurezza è indicativo di una violazione della legge che richiede azioni legali specifiche.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0110	Identifica e/o determina se un incidente di sicurezza è indicativo di una violazione della legge che richiede azioni legali specifiche.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0128	Integra, laddove possibile, funzionalità automatizzate per l'aggiornamento del software di sistema o l'applicazione di patch allo stesso e sviluppa processi e procedure per l'aggiornamento e l'applicazione di patch manuali in base ai requisiti di tempistica delle patch attuali e previsti per l'ambiente operativo del sistema.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0128	Integra, laddove possibile, funzionalità automatizzate per l'aggiornamento del software di sistema o l'applicazione di patch allo stesso e sviluppa processi e procedure per l'aggiornamento e l'applicazione di patch manuali in base ai requisiti di tempistica delle patch attuali e previsti per l'ambiente operativo del sistema.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0128	Integra, laddove possibile, funzionalità automatizzate per l'aggiornamento del software di sistema o l'applicazione di patch allo stesso e sviluppa processi e procedure per l'aggiornamento e l'applicazione di patch manuali in base ai requisiti di tempistica delle patch attuali e previsti per l'ambiente operativo del sistema.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0128	Integra, laddove possibile, funzionalità automatizzate per l'aggiornamento del software di sistema o l'applicazione di patch allo stesso e sviluppa processi e procedure per l'aggiornamento e l'applicazione di patch manuali in base ai requisiti di tempistica delle patch attuali e previsti per l'ambiente operativo del sistema.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecch iature.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecch iature.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecch iature.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon Elasticsearch Service (Amazon ES) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon ES all'interno di un Amazon VPC permette la comunicazione sicura tra Amazon ES e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.
T0144	Gestisci account, diritti di rete e accesso a sistemi e apparecchiature.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0151	Monitora e valuta l'efficacia delle misure di cibersicu rezza dell'azienda per garantire che forniscano il livello di protezione previsto.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0151	Monitora e valuta l'efficacia delle misure di cibersicu rezza dell'azienda per garantire che forniscano il livello di protezione previsto.	cloudwatch-alarm-a ction-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazio ne. L'allarme esegue una o più operazion i basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazion i di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0151	Monitora e valuta l'efficacia delle misure di cibersicu rezza dell'azienda per garantire che forniscano il livello di protezione previsto.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorar e la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
T0152	Monitora e gestisci i database per garantire prestazioni ottimali.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0153	Monitora la capacità e le prestazioni della rete.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0153	Monitora la capacità e le prestazioni della rete.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
T0153	Monitora la capacità e le prestazioni della rete.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0153	Monitora la capacità e le prestazioni della rete.	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorar e la disponibilità di Amazon RDS. Ciò fornisce una visibilit à dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archivi azione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositi vo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0154	Monitora e segnala l'utilizzo delle risorse e degli asset per la gestione delle conoscenze.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
T0156	Supervisiona la gestione della configurazione e formula raccomand azioni al riguardo.	account-part-of-organizations	La gestione centraliz zata Account AWS all'interno di AWS Organizations aiuta a garantire la conformit à degli account. L'assenza di una governance centraliz zata degli account può comportar e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0156	Supervisiona la gestione della configurazione e formula raccomand azioni al riguardo.	ec2-instance-manag ed-by-systems-mana ger	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0156	Supervisiona la gestione della configurazione e formula raccomandazioni al riguardo.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0156	Supervisiona la gestione della configurazione e formula raccomand azioni al riguardo.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0156	Supervisiona la gestione della configurazione e formula raccomand azioni al riguardo.	redshift-cluster-m aintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizza zione. In particola re, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVers ionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltati vamente il preferred MaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotR etention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0156	Supervisiona la gestione della configurazione e formula raccomand azioni al riguardo.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0156	Supervisiona la gestione della configurazione e formula raccomand azioni al riguardo.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0156	Supervisiona la gestione della configurazione e formula raccomand azioni al riguardo.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0156	Supervisiona la gestione della configurazione e formula raccomand azioni al riguardo.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0160	Correggi le vulnerabilità della rete per garantire che le informazioni siano protette da terze parti.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0160	Correggi le vulnerabilità della rete per garantire che le informazioni siano protette da terze parti.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0160	Correggi le vulnerabilità della rete per garantire che le informazioni siano protette da terze parti.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0162	Esegui il backup e il ripristino dei database per garantire l'integrità dei dati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0166	Esegui la correlazione degli eventi utilizzando le informazioni raccolte da diverse fonti all'interno dell'azienda per acquisire consapevolezza della situazione e determinare l'efficacia di un attacco osservato.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0168	Esegui il confronto degli hash rispetto al database stabilito.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon Elasticsearch Service (Amazon ES) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon ES all'interno di un Amazon VPC permette la comunicazione sicura tra Amazon ES e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazi oni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0195	Fornisci un flusso gestito di informazioni pertinenti (tramite portali basati sul Web o altri mezzi) a seconda dei requisiti della missione.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0215	Riconosci una possibile violazion e della sicurezza e intraprendi le azioni appropriate per segnalare l'incidente, come richiesto.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0244	Verifica che i livelli di sicurezza del software applicativo, della rete e del sistema siano implement ati come indicato, documenta le deviazioni e suggerisc i le azioni necessari e per correggere tali deviazioni.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integri tà dei log. CloudTrai l La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificar e, eliminare o falsifica re i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0244	Verifica che i livelli di sicurezza del software applicativo, della rete e del sistema siano implementati come indicato, documenta le deviazioni e suggerisci le azioni necessarie per correggere tali deviazioni.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0244	Verifica che i livelli di sicurezza del software applicativo, della rete e del sistema siano implementati come indicato, documenta le deviazioni e suggerisci le azioni necessarie per correggere tali deviazioni.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0258	Ottieni rilevamento, identificazione e segnalazione tempestivi di possibili attacchi/intrusioni, attività anomale e attività di uso improprio e distingui questi incidenti ed eventi da attività benigne.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0259	Utilizza strumenti di difesa informatica per il monitoraggio e l'analisi continui dell'attività del sistema per identific are attività dannose.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	alb-waf-enabled	Assicurati che il AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	api-gw-associated-with-waf	AWS WAF consente di configurare una serie di regole (denominate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon Elasticsearch Service (Amazon ES) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon ES all'interno di un Amazon VPC permette la comunicazione sicura tra Amazon ES e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0262	Utilizza defense-in-depth principi e pratiche approvati (ad esempio, defense-in-multiple luoghi, difese a più livelli, robustezza della sicurezza).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	iam-policy-no-stat ements-with-full-a ccess	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	rds-automatic-mino r-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'install azione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relaziona le (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'eliminazione dei punti di ripristino può aiutare a prevenire l'eliminazione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundatio

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			nal Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicuran doti che i domini Amazon Elasticse arch Service (Amazon ES) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon ES all'inter no di un Amazon VPC permette la comunicazione sicura tra Amazon ES e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0284	Progetta e sviluppa nuovi strumenti/ tecnologie relativi alla cibersicurezza.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0306	Supporta la gestione degli incidenti, dei livelli di servizio, delle modifiche, delle release, della continuità e della disponibilità per i database e i sistemi di gestione dei dati.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0306	Supporta la gestione degli incidenti, dei livelli di servizio, delle modifiche, delle release, della continuità e della disponibilità per i database e i sistemi di gestione dei dati.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0306	Supporta la gestione degli incidenti, dei livelli di servizio, delle modifiche, delle release, della continuità e della disponibilità per i database e i sistemi di gestione dei dati.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0314	Sviluppa un contesto di sicurezza del sistema, un Concept of Operations (CONOPS) preliminare per la sicurezza del sistema, e definisci i requisiti di sicurezza del sistema di base in conformità ai requisiti di cibersicurezza applicabili.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0314	Sviluppa un contesto di sicurezza del sistema, un Concept of Operations (CONOPS) preliminare per la sicurezza del sistema, e definisci i requisiti di sicurezza del sistema di base in conformità ai requisiti di cibersicurezza applicabili.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0314	Sviluppa un contesto di sicurezza del sistema, un Concept of Operations (CONOPS) preliminare per la sicurezza del sistema, e definisci i requisiti di sicurezza del sistema di base in conformità ai requisiti di cibersicurezza applicabili.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0314	Sviluppa un contesto di sicurezza del sistema, un Concept of Operations (CONOPS) preliminare per la sicurezza del sistema, e definisci i requisiti di sicurezza del sistema di base in conformità ai requisiti di cibersicurezza applicabili.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0314	Sviluppa un contesto di sicurezza del sistema, un Concept of Operations (CONOPS) preliminare per la sicurezza del sistema, e definisci i requisiti di sicurezza del sistema di base in conformità ai requisiti di cibersicurezza applicabili.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0314	Sviluppa un contesto di sicurezza del sistema, un Concept of Operations (CONOPS) preliminare per la sicurezza del sistema, e definisci i requisiti di sicurezza del sistema di base in conformità ai requisiti di cibersicurezza applicabili.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0333	Esegui l'analisi delle tendenze nella difesa informatica e crea i relativi report.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0333	Esegui l'analisi delle tendenze nella difesa informatica e crea i relativi report.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0347	Valuta la validità dei dati di origine e dei risultati successivi.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0358	Progetta e sviluppa funzionalità di amministrazione e gestione del sistema per gli utenti con accesso con privilegi.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
T0358	Progetta e sviluppa funzionalità di amministrazione e gestione del sistema per gli utenti con accesso con privilegi.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0358	Progetta e sviluppa funzionalità di amministrazione e gestione del sistema per gli utenti con accesso con privilegi.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0358	Progetta e sviluppa funzionalità di amministrazione e gestione del sistema per gli utenti con accesso con privilegi.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0358	Progetta e sviluppa funzionalità di amministrazione e gestione del sistema per gli utenti con accesso con privilegi.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
T0358	Progetta e sviluppa funzionalità di amministrazione e gestione del sistema per gli utenti con accesso con privilegi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0358	Progetta e sviluppa funzionalità di amministrazione e gestione del sistema per gli utenti con accesso con privilegi.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
T0358	Progetta e sviluppa funzionalità di amministrazione e gestione del sistema per gli utenti con accesso con privilegi.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformit à ai requisiti dell'orga nizzazione.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformit à ai requisiti dell'orga nizzazione.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformità ai requisiti dell'organizzazione.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformità ai requisiti dell'organizzazione.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformità ai requisiti dell'organizzazione.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformit à ai requisiti dell'orga nizzazione.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformit à ai requisiti dell'orga nizzazione.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformit à ai requisiti dell'orga nizzazione.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformit à ai requisiti dell'orga nizzazione.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformità ai requisiti dell'organizzazione.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformit à ai requisiti dell'orga nizzazione.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformità ai requisiti dell'organizzazione.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformità ai requisiti dell'organizzazione.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformità ai requisiti dell'organizzazione.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformità ai requisiti dell'organizzazione.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformità ai requisiti dell'organizzazione.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformità ai requisiti dell'organizzazione.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformità ai requisiti dell'organizzazione.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0376	Istituisci programmi di gestione della forza lavoro informatica, fornisci le relative risorse, implementali e valutali in conformità ai requisiti dell'organizzazione.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0416	Abilita le applicazioni con chiave pubblica sfruttando le librerie di infrastrutture a chiave pubblica (PKI) esistenti e incorporando funzionalità di crittografia e gestione dei certificati, laddove opportuno.	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da AWS ACM. Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
T0416	Abilita le applicazioni con chiave pubblica sfruttando le librerie di infrastrutture a chiave pubblica (PKI) esistenti e incorporando funzionalità di crittografia e gestione dei certificati, laddove opportuno.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0416	Abilita le applicazioni con chiave pubblica sfruttando le librerie di infrastrutture a chiave pubblica (PKI) esistenti e incorpora ndo funzionalità di crittografia e gestione dei certificati, laddove opportuno.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0416	Abilita le applicazioni con chiave pubblica sfruttando le librerie di infrastrutture a chiave pubblica (PKI) esistenti e incorpora ndo funzionalità di crittografia e gestione dei certificati, laddove opportuno.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
T0416	Abilita le applicazioni con chiave pubblica sfruttando le librerie di infrastrutture a chiave pubblica (PKI) esistenti e incorpora ndo funzionalità di crittografia e gestione dei certificati, laddove opportuno.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0416	Abilita le applicazioni con chiave pubblica sfruttando le librerie di infrastrutture a chiave pubblica (PKI) esistenti e incorpora ndo funzionalità di crittografia e gestione dei certificati, laddove opportuno.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
T0416	Abilita le applicazioni con chiave pubblica sfruttando le librerie di infrastrutture a chiave pubblica (PKI) esistenti e incorpora ndo funzionalità di crittografia e gestione dei certificati, laddove opportuno.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0416	Abilita le applicazioni con chiave pubblica sfruttando le librerie di infrastrutture a chiave pubblica (PKI) esistenti e incorporando funzionalità di crittografia e gestione dei certificati, laddove opportuno.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
T0416	Abilita le applicazioni con chiave pubblica sfruttando le librerie di infrastrutture a chiave pubblica (PKI) esistenti e incorporando funzionalità di crittografia e gestione dei certificati, laddove opportuno.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0416	Abilita le applicazioni con chiave pubblica sfruttando le librerie di infrastrutture a chiave pubblica (PKI) esistenti e incorporando funzionalità di crittografia e gestione dei certificati, laddove opportuno.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
T0421	Gestisci l'indicizzazione/catalogazione, l'archiviazione e l'accesso a conoscenze organizzative esplicite (ad esempio documenti cartacei, file digitali).	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0421	Gestisci l'indicizzazione/catalogazione, l'archiviazione e l'accesso a conoscenze organizzative esplicite (ad esempio, documenti cartacei, file digitali).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0421	Gestisci l'indicizzazione/catalogazione, l'archiviazione e l'accesso a conoscenze organizzative esplicite (ad esempio documenti cartacei, file digitali).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0421	Gestisci l'indicizzazione/catalogazione, l'archiviazione e l'accesso a conoscenze organizzative esplicite (ad esempio documenti cartacei, file digitali).	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0421	Gestisci l'indicizzazione/catalogazione, l'archiviazione e l'accesso a conoscenze organizzative esplicite (ad esempio documenti cartacei, file digitali).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0421	Gestisci l'indicizzazione/catalogazione, l'archiviazione e l'accesso a conoscenze organizzative esplicite (ad esempio documenti cartacei, file digitali).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.
T0421	Gestisci l'indicizzazione/catalogazione, l'archiviazione e l'accesso a conoscenze organizzative esplicite (ad esempio documenti cartacei, file digitali).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0421	Gestisci l'indiciz zazione/catalogazi one, l'archiviazione e l'accesso a conoscenze organizza tive esplicite (ad esempio documenti cartacei, file digitali).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
T0421	Gestisci l'indiciz zazione/catalogazi one, l'archiviazione e l'accesso a conoscenze organizza tive esplicite (ad esempio documenti cartacei, file digitali).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0421	Gestisci l'indicizzazione/catalogazione, l'archiviazione e l'accesso a conoscenze organizzative esplicite (ad esempio documenti cartacei, file digitali).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0421	Gestisci l'indiciz zazione/catalogazi one, l'archiviazione e l'accesso a conoscenze organizza tive esplicite (ad esempio documenti cartacei, file digitali).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
T0421	Gestisci l'indiciz zazione/catalogazi one, l'archiviazione e l'accesso a conoscenze organizza tive esplicite (ad esempio documenti cartacei, file digitali).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0421	Gestisci l'indicizzazione/catalogazione, l'archiviazione e l'accesso a conoscenze organizzative esplicite (ad esempio documenti cartacei, file digitali).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0421	Gestisci l'indiciz zazione/catalogazi one, l'archiviazione e l'accesso a conoscenze organizza tive esplicite (ad esempio documenti cartacei, file digitali).	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
T0421	Gestisci l'indicizzazione/catalogazione, l'archiviazione e l'accesso a conoscenze organizzative esplicite (ad esempio, documenti cartacei, file digitali).	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0421	Gestisci l'indicizzazione/catalogazione, l'archiviazione e l'accesso a conoscenze organizzative esplicite (ad esempio documenti cartacei, file digitali).	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
T0475	Valuta i controlli di accesso adeguati sulla base dei principi del privilegio minimo e. need-to-know	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati sulla base dei principi del privilegio minimo e. need-to-know	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati sulla base dei principi del privilegio minimo e. need-to-know	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati sulla base dei principi del privilegio minimo e. need-to-know	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
T0475	Valuta i controlli di accesso adeguati sulla base dei principi del privilegio minimo e. need-to-know	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e need-to-know.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicuran doti che i domini Amazon Elasticse arch Service (Amazon ES) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon ES all'inter no di un Amazon VPC permette la comunicazione sicura tra Amazon ES e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
T0475	Valuta i controlli di accesso adeguati in base ai principi del privilegio minimo e. need-to-know	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0489	Implementa misure di sicurezza del sistema in conformità alle procedure stabilite per garantire riservatezza, integrità, disponibilità, autenticazione e non ripudio.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0489	Implementa misure di sicurezza del sistema in conformità alle procedure stabilite per garantire riservatezza, integrità, disponibilità, autenticazione e non ripudio.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0489	Implementa misure di sicurezza del sistema in conformità alle procedure stabilite per garantire riservatezza, integrità, disponibilità, autenticazione e non ripudio.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
T0489	Implementa misure di sicurezza del sistema in conformità alle procedure stabilite per garantire riservatezza, integrità, disponibilità, autenticazione e non ripudio.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0489	Implementa misure di sicurezza del sistema in conformità alle procedure stabilite per garantire riservatezza, integrità, disponibilità, autenticazione e non ripudio.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
T0489	Implementa misure di sicurezza del sistema in conformità alle procedure stabilite per garantire riservatezza, integrità, disponibilità, autenticazione e non ripudio.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0489	Implementa misure di sicurezza del sistema in conformità alle procedure stabilite per garantire riservatezza, integrità, disponibilità, autenticazione e non ripudio.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0489	Implementa misure di sicurezza del sistema in conformità alle procedure stabilite per garantire riservatezza, integrità, disponibilità, autenticazione e non ripudio.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0489	Implementa misure di sicurezza del sistema in conformità alle procedure stabilite per garantire riservatezza, integrità, disponibilità, autenticazione e non ripudio.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0489	Implementa misure di sicurezza del sistema in conformità alle procedure stabilite per garantire riservatezza, integrità, disponibilità, autenticazione e non ripudio.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0489	Implementa misure di sicurezza del sistema in conformità alle procedure stabilite per garantire riservatezza, integrità, disponibilità, autenticazione e non ripudio.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0489	Implementa misure di sicurezza del sistema in conformità alle procedure stabilite per garantire riservatezza, integrità, disponibilità, autenticazione e non ripudio.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0491	Installa e configura hardware, software e apparecchiature periferiche per gli utenti del sistema in conformità agli standard dell'organizzazione.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0491	Installa e configura hardware, software e apparecchiature periferiche per gli utenti del sistema in conformità agli standard dell'organizzazione.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0491	Installa e configura hardware, software e apparecchiature periferiche per gli utenti del sistema in conformità agli standard dell'orga nizzazione.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0503	Monitora le fonti di dati esterne (ad esempio, i siti dei fornitori di servizi di difesa informatica, i Computer Emergency Response Teams, Security Focus) per tenere sotto controllo le condizioni delle minacce alla difesa informatica e determinare quali problemi di sicurezza possono avere un impatto sull'azienda.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
T0509	Esegui una valutazione del rischio per la sicurezza delle informazioni.	annual-risk-assessment-performed (controllo del processo)	Esegui una valutazione annuale del rischio sulla tua organizzazione. Le valutazioni del rischio possono aiutare a determinare la probabilità e l'impatto dei rischi e/o delle vulnerabilità identificati che interessano un'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon Elasticsearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica funzioni di sicurezza informatica (ad esempio crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica funzioni di sicurezza informatica (ad esempio crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	opensearch-encrypted-at-rest	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i domini Amazon Elasticsearch Service (Amazon ES).
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon Elasticsearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica funzioni di sicurezza informatica (ad esempio crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	elasticsearch-encrypted-at-rest	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i domini Amazon Elasticsearch Service (Amazon ES).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
T0553	Applica funzioni di sicurezza informatica (ad esempio crittografia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittogra fia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
T0553	Applica funzioni di sicurezza informatica (ad esempio crittogra fia, controllo degli accessi e gestione delle identità) per ridurre le opportunità di sfruttamento.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0553	Applica le funzioni di sicurezza informatica (ad esempio, crittografia, controllo degli accessi e gestione dell'identità) per ridurre le opportunità di sfruttamento.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
T0557	Integra le funzioni di gestione delle chiavi relative al ciberspazio.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che vengano ruotate una volta terminato il loro periodo di crittografia.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0557	Integra le funzioni di gestione delle chiavi relative al ciberspazio.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0576	Valuta l'intelligence proveniente da tutte le fonti e raccomand a le destinazioni per supportare gli obiettivi delle operazioni informatiche.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon Elasticsearch Service (Amazon ES) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon ES all'interno di un Amazon VPC permette la comunicazione sicura tra Amazon ES e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon Elasticsearch Service (Amazon ES) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon ES all'interno di un Amazon VPC permette la comunicazione sicura tra Amazon ES e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
T0609	Abilita l'accesso ai computer wireless e alle reti digitali.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0616	Esegui l'esplorazione della rete e l'analisi delle vulnerabilità dei sistemi all'interno di una rete.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0686	Identifica le vulnerabilità alle minacce.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0686	Identifica le vulnerabilità alle minacce.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	elasticsearch-logs-to-cloudwatch	Assicurati che i domini del servizio Amazon Elasticsearch abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	lambda-dlq-check	Abilita questa regola per avvisare il personale appropriato tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0706	Raccogli informazioni sulle reti attraverso tecniche tradizionali e alternative (ad esempio, analisi dei social network, concatenamento delle chiamate, analisi del traffico).	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0777	Crea un profilo degli amministratori di rete o di sistema e delle loro attività.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0805	Segnala eventi e intrusioni di rete significativi derivati dall'intelligence.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
T0877	Collabora con le unità dell'organizzazion i competenti per supervisionare i diritti di accesso alle informazioni dei consumatori.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0877	Collabora con le unità dell'organizzazioni competenti per supervisionare i diritti di accesso alle informazioni dei consumatori.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0877	Collabora con le unità dell'organizzazion i competenti per supervisionare i diritti di accesso alle informazioni dei consumatori.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
T0877	Collabora con le unità dell'organizzazion i competenti per supervisionare i diritti di accesso alle informazioni dei consumatori.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0877	Collabora con le unità dell'organizzazioni competenti per supervisionare i diritti di accesso alle informazioni dei consumatori.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0877	Collabora con le unità dell'organizzazion i competenti per supervisionare i diritti di accesso alle informazioni dei consumatori.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
T0877	Collabora con le unità dell'organizzazion i competenti per supervisionare i diritti di accesso alle informazioni dei consumatori.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0877	Collabora con le unità dell'organizzazioni competenti per supervisionare i diritti di accesso alle informazioni dei consumatori.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0877	Collabora con le unità dell'organizzazioni competenti per supervisionare i diritti di accesso alle informazioni dei consumatori.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
T0877	Collabora con le unità dell'organizzazioni competenti per supervisionare i diritti di accesso alle informazioni dei consumatori.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0877	Collabora con le unità dell'organizzazion i competenti per supervisionare i diritti di accesso alle informazioni dei consumatori.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0935	Esegui una valutazione del rischio per la sicurezza delle informazioni.	annual-risk-assessment-performed (controllo del processo)	Esegui una valutazione annuale del rischio sulla tua organizzazione. Le valutazioni del rischio possono aiutare a determinare la probabilità e l'impatto dei rischi e/o delle vulnerabilità identificati che interessano un'organizzazione.
T0960	Monitora le modifiche apportate a un sistema e al suo ambiente operativo.	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0960	Monitora le modifiche apportate a un sistema e al suo ambiente operativo.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0960	Monitora le modifiche apportate a un sistema e al suo ambiente operativo.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0960	Monitora le modifiche apportate a un sistema e al suo ambiente operativo.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0960	Monitora le modifiche apportate a un sistema e al suo ambiente operativo.	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0960	Monitora le modifiche apportate a un sistema e al suo ambiente operativo.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0960	Monitora le modifiche apportate a un sistema e al suo ambiente operativo.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
T0960	Monitora le modifiche apportate a un sistema e al suo ambiente operativo.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegio minimo e della separazione dei compiti, abilitando Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuare l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuzione delle chiavi (KDC). Fornisce un mezzo per l'autenticazione dei principali. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundatio

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			nal Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0992	Determina il modo in cui verranno utilizzati i risultati del monitoraggio continuo nell'autorizzazione continua.	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	iam-user-group-membership-check	AWS Identity and Access Managemen t (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicuran do che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
T0993	Stabilisci processi e procedure di controllo degli accessi a strumenti e tecnologi e di monitoraggio continuo.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NIST 800 181.

Best practice operative per NIST 1800 25

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra NIST 1800-25 e AWS le regole Config gestite. Ciascuna AWS Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli NIST

1800-25. Un controllo NIST 1800-25 può essere correlato a più regole. AWS Config Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.AM-2	Le applicazioni e le piattaforme software all'interno dell'organizzazione vengono inventariate	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
ID.AM-2	Le applicazioni e le piattaforme software all'interno dell'organizzazione vengono inventariate	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organi

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			zzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.
ID.AM-2	Le applicazioni e le piattaforme software all'interno dell'organizzazione vengono inventariate	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.AM-2	Le applicazioni e le piattaforme software all'interno dell'orga nizzazione vengono inventariate	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.
ID.AM-2	Le applicazioni e le piattaforme software all'interno dell'orga nizzazione vengono inventariate	vpc-network-acl-un used-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventari o e una gestione accurati del proprio ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-1	Le vulnerabilità degli asset vengono identificate e documentate	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-1	Le vulnerabilità degli asset vengono identificate e documentate	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-1	Le vulnerabilità degli asset vengono identificate e documentate	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-1	Le vulnerabilità degli asset vengono identificate e documentate	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.
PR.AC-3	Viene gestito l'accesso remoto.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
PR.AC-3	Viene gestito l'accesso remoto.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-3	Viene gestito l'accesso remoto.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-3	Viene gestito l'accesso remoto.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-3	Viene gestito l'accesso remoto.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
PR.AC-3	Viene gestito l'accesso remoto.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.AC-3	Viene gestito l'accesso remoto.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D è protetto ata-at-rest	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
PR.DS-1	D ata-at-rest è protetto	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
PR.DS-1	D ata-at-rest è protetto	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
PR.DS-1	D è protetto ata-at-re st	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
PR.DS-1	D ata-at-rest è protetto	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
PR.DS-1	D ata-at-rest è protetto	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
PR.DS-1	D ata-at-rest è protetto	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D è protetto ata-at-rest	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
PR.DS-1	D ata-at-rest è protetto	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D è protetto ata-at-rest	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
PR.DS-1	D è protetto ata-at-rest	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
PR.DS-1	D ata-at-rest è protetto	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-2	D ata-in-transit è protetto	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-2	D è protetto ata-in-transit	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
PR.DS-2	D è protetto ata-in-transit	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-2	D ata-in-transit è protetto	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
PR.DS-2	D è protetto ata-in-transit	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-2	D ata-in-transit è protetto	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
PR.DS-2	D ata-in-transit è protetto	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-2	D è protetto ata-in-transit	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
PR.DS-2	D ata-in-transit è protetto	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-6	I meccanismi di controllo dell'integrità vengono utilizzati per verificare l'integrità del software, del firmware e delle informazioni	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-6	I meccanismi di controllo dell'integrità vengono utilizzati per verificare l'integrità del software, del firmware e delle informazioni	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione e dei sistemi di controllo industriale che incorpora i principi di sicurezza (ad esempio il concetto di minima funzionalità)	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione e dei sistemi di controllo industriale che incorpora i principi di sicurezza (ad esempio il concetto di minima funzionalità)	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione e dei sistemi di controllo industriale che incorpora principi di sicurezza (ad esempio il concetto di minima funzionalità)	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione e dei sistemi di controllo industriale che incorpora principi di sicurezza (ad esempio il concetto di minima funzionalità)	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione e dei sistemi di controllo industriale che incorpora i principi di sicurezza (ad esempio il concetto di minima funzionalità)	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione e dei sistemi di controllo industriale che incorpora i principi di sicurezza (ad esempio il concetto di minima funzionalità)	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-3	I processi di controllo delle modifiche alla configurazione sono predisposti	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-3	I processi di controllo delle modifiche alla configurazione sono predisposti	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-9	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) sono attivati e gestiti.	response-plan-exists-maintained (Controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsabile di piani di risposta agli incidenti. Disporre di piani di risposta aggiornati e formalmente documentati può aiutare a garantire che il personale addetto all'intervento comprenda ruoli, responsabilità e processi da seguire durante un incidente.
PR.IP-10	I piani di risposta e ripristino vengono testati.	response-plan-tested (Controllo del processo)	Verifica che i piani di risposta agli incidenti e di ripristino siano testati. Questo può aiutare a capire se il piano sarà efficace in caso di incidente e se è necessario risolvere eventuali lacune o apportare aggiornamenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-12	Viene sviluppato e implementato un piano di gestione delle vulnerabilità.	vuln-management-plan-exists (Controllo del processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente. Ciò può includere strumenti di gestione delle vulnerabilità, cadenza di scansione ambientale, ruoli e responsabilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-12	Viene sviluppato e implementato un piano di gestione delle vulnerabilità	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-12	Viene sviluppato e implementato un piano di gestione delle vulnerabilità	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-12	Viene sviluppato e implementato un piano di gestione delle vulnerabilità	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.MA-2	La manutenzione remota delle risorse dell'organizzazione e viene approvata, registrata ed eseguita in modo da impedire l'accesso non autorizzato	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.MA-2	La manutenzione remota delle risorse dell'organizzazion e viene approvata , registrata ed eseguita in modo da impedire l'accesso non autorizzato	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	Le reti di comunicazione e controllo sono protette	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzional ità viene incorpora to configurando i sistemi in modo da fornire solo funzional ità essenziali	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'inter no del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzional ità viene incorpora to configurando i sistemi in modo da fornire solo funzional ità essenziali	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
PR.PT-4	Le reti di comunicazione e controllo sono protette	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	acm-certificate-expiration-check	Assicurati che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
PR.PT-4	Le reti di comunicazione e controllo sono protette	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-4	Le reti di comunicazione e controllo sono protette	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-4	Le reti di comunicazione e controllo sono protette	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-4	Le reti di comunicazione e controllo sono protette	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.PT-4	Le reti di comunicazione e controllo sono protette	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
PR.PT-4	Le reti di comunicazione e controllo sono protette	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-8	Vengono eseguite scansioni di vulnerabilità.	vuln-scans-performed (Controllo del processo)	Assicurati che le scansioni delle vulnerabilità vengano eseguite in base ai requisiti di conformità. La cadenza di scansione, gli strumenti utilizzati e l'uso dei risultati devono essere definiti dall'organizzazione.
RS.MI-3	Le vulnerabilità appena identificate vengono mitigate o documentate come rischi accettati.	vuln-mitigated-accepted (Controllo del processo)	Assicurati che le vulnerabilità appena identificate vengano corrette o documentate come rischi accettati. Servizi come AWS Security Hub, Amazon Guard Duty, Amazon Inspector e AWS Config possono aiutarti a identificare le vulnerabilità all'interno del tuo ambiente. Le vulnerabilità devono essere corrette o accettate come rischi in base ai requisiti di conformità dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.MI-3	Le vulnerabilità appena identificate vengono mitigate o documentate come rischi accettati	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NIST 1800 25.

Best practice operative per NIST CSF

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità,

in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il NIST Cyber Security Framework (CSF) e le regole Config gestite AWS . Ogni AWS Config regola si applica a una AWS risorsa specifica e si riferisce a uno o più controlli NIST CSF. Un controllo NIST CSF può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-1	Viene stabilita e gestita una linea di base delle operazioni di rete e dei flussi di dati previsti per utenti e sistemi	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-2	Gli eventi rilevati vengono analizzati per comprendere obiettivi e metodi di attacco	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-2	Gli eventi rilevati vengono analizzat i per comprendere obiettivi e metodi di attacco	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-3	I dati sugli eventi vengono raccolti e messi in correlazione da più fonti e sensori	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
DE.AE-4	Viene stabilito l'impatto degli eventi	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-4	Viene stabilito l'impatto degli eventi	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registran do le azioni della Console di gestione e le chiamate API. AWS È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-4	Viene stabilito l'impatto degli eventi	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-4	Viene stabilito l'impatto degli eventi	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-4	Viene stabilito l'impatto degli eventi	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-4	Viene stabilito l'impatto degli eventi	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-4	Viene stabilito l'impatto degli eventi	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.AE-4	Viene stabilito l'impatto degli eventi	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-1	La rete viene monitorata per rilevare potenziali eventi di cibersicurezza	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
DE.CM-1	La rete viene monitorata per rilevare potenziali eventi di cibersicurezza	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-1	La rete viene monitorata per rilevare potenziali eventi di cibersicurezza	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-1	La rete viene monitorata per rilevare potenziali eventi di cibersicurezza	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-1	La rete viene monitorata per rilevare potenziali eventi di cibersicu rezza	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-1	La rete viene monitorata per rilevare potenziali eventi di cibersicu rezza	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-1	La rete viene monitorata per rilevare potenziali eventi di cibersicurezza	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-1	La rete viene monitorata per rilevare potenziali eventi di cibersicurezza	s3-event-notifications-enabled	Le notifiche degli eventi di Amazon S3 possono notificare al personale competente eventuali modifiche accidentali o intenzionali agli oggetti del bucket. Gli avvisi includono: creazione di un nuovo oggetto, rimozione di oggetti, ripristino di oggetti, oggetti persi e replicati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-1	La rete viene monitorata per rilevare potenziali eventi di cibersicurezza	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-1	La rete viene monitorata per rilevare potenziali eventi di cibersicu rezza	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
DE.CM-3	L'attività del personale viene monitorata per rilevare potenziali eventi di cibersicu rezza	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-3	L'attività del personale viene monitorata per rilevare potenziali eventi di cibersicu rezza	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registran do le azioni della Console di gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-3	L'attività del personale viene monitorata per rilevare potenziali eventi di cibersicu rezza	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-3	L'attività del personale viene monitorata per rilevare potenziali eventi di cibersicu rezza	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-3	L'attività del personale viene monitorata per rilevare potenziali eventi di cibersicu rezza	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-3	L'attività del personale viene monitorata per rilevare potenziali eventi di cibersicu rezza	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-4	Viene rilevato il codice dannoso	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-4	Viene rilevato il codice dannoso	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-5	Viene rilevato il codice mobile non autorizzato	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
DE.CM-5	Viene rilevato il codice mobile non autorizzato	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-5	Viene rilevato il codice mobile non autorizzato	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-5	Viene rilevato il codice mobile non autorizzato	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-5	Viene rilevato il codice mobile non autorizzato	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-5	Viene rilevato il codice mobile non autorizzato	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-6	L'attività dei fornitori di servizi esterni viene monitorata per rilevare potenziali eventi di cibersicu rezza	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazi oni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-6	L'attività dei fornitori di servizi esterni viene monitorata per rilevare potenziali eventi di cibersicu rezza	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registran do le azioni della Console di gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-6	L'attività dei fornitori di servizi esterni viene monitorata per rilevare potenziali eventi di cibersicu rezza	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-6	L'attività dei fornitori di servizi esterni viene monitorata per rilevare potenziali eventi di cibersicu rezza	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-6	L'attività dei fornitori di servizi esterni viene monitorata per rilevare potenziali eventi di cibersicu rezza	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorar e la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorat i mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinent e.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-6	L'attività dei fornitori di servizi esterni viene monitorata per rilevare potenziali eventi di cibersicu rezza	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-7	Viene eseguito il monitoraggio di personale, connessioni, dispositivi e software non autorizzati	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
DE.CM-7	Viene eseguito il monitoraggio di personale, connessioni, dispositivi e software non autorizzati	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-7	Viene eseguito il monitoraggio di personale, connessioni, dispositivi e software non autorizzati	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-7	Viene eseguito il monitoraggio di personale, connessioni, dispositivi e software non autorizzati	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-7	Viene eseguito il monitoraggio di personale, connessioni, dispositivi e software non autorizzati	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-7	Viene eseguito il monitoraggio di personale, connessioni, dispositivi e software non autorizzati	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-7	Viene eseguito il monitoraggio di personale, connessioni, dispositivi e software non autorizzati	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-7	Viene eseguito il monitoraggio di personale, connessioni, dispositivi e software non autorizzati	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.CM-7	Viene eseguito il monitoraggio di personale, connessioni, dispositivi e software non autorizzati	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.DP-4	Vengono comunicate le informazioni sul rilevamento degli eventi	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
DE.DP-4	Vengono comunicate le informazioni sul rilevamento degli eventi	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.DP-4	Vengono comunicate le informazioni sul rilevamento degli eventi	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.DP-4	Vengono comunicate le informazioni sul rilevamento degli eventi	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.DP-4	Vengono comunicate le informazioni sul rilevamento degli eventi	s3-event-notifications-enabled	Le notifiche degli eventi di Amazon S3 possono notificare al personale competente eventuali modifiche accidentali o intenzionali agli oggetti del bucket. Gli avvisi includono: creazione di un nuovo oggetto, rimozione di oggetti, ripristino di oggetti, oggetti persi e replicati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.DP-4	Vengono comunicate le informazioni sul rilevamento degli eventi	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.DP-4	Vengono comunicate le informazioni sul rilevamento degli eventi	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
DE.DP-5	I processi di rilevamento vengono migliorati continuamente	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.AM-2	Le applicazioni e le piattaforme software all'interno dell'orga nizzazione vengono inventariate	ec2-instance-manag ed-by-systems-mana ger	Un inventario delle piattaforme software e delle applicazioni all'interno dell'orga nizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configura zioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installaz ioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambi ente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.AM-2	Le applicazioni e le piattaforme software all'interno dell'organizzazione vengono inventariate	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.AM-2	Le applicazioni e le piattaforme software all'interno dell'orga nizzazione vengono inventariate	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.
ID.AM-2	Le applicazioni e le piattaforme software all'interno dell'orga nizzazione vengono inventariate	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.AM-2	Le applicazioni e le piattaforme software all'interno dell'organizzazione vengono inventariate	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.
ID.AM-3	Vengono mappati i flussi di dati e le comunicazioni dell'organizzazione	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.AM-3	Vengono mappati i flussi di dati e le comunicazioni dell'organizzazione	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.AM-3	Vengono mappati i flussi di dati e le comunicazioni dell'organizzazione	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.AM-3	Vengono mappati i flussi di dati e le comunicazioni dell'organizzazione	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.AM-3	Vengono mappati i flussi di dati e le comunicazioni dell'organizzazione	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.AM-3	Vengono mappati i flussi di dati e le comunicazioni dell'organizzazione	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.AM-3	Vengono mappati i flussi di dati e le comunicazioni dell'organizzazione	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.BE-5	I requisiti di resilienza per supportare la fornitura di servizi critici sono stabiliti per tutti gli stati operativi (ad esempio in caso di costrizione/attacco, durante il ripristino, durante le normali operazioni)	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-1	Le vulnerabilità degli asset vengono identificate e documentate	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-1	Le vulnerabilità degli asset vengono identificate e documentate	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-1	Le vulnerabilità degli asset vengono identificate e documentate	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornam enti, correzioni e funzionalità disponibi li per l'ambiente. Rimanere costantem ente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-1	Le vulnerabilità degli asset vengono identificate e documentate	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-2	Le informazioni sulle minacce informati che vengono ricevute da forum e fonti di condivisione delle informazioni	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-3	Le minacce, sia interne che esterne, vengono identificate e documentate	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-3	Le minacce, sia interne che esterne, vengono identificate e documentate	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
ID.RA-5	Minacce, vulnerabilità, probabilità e impatti vengono utilizzati per determinare il rischio	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-5	Minacce, vulnerabilità, probabilità e impatti vengono utilizzati per determinare il rischio	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-5	Minacce, vulnerabilità, probabilità e impatti vengono utilizzati per determinare il rischio	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.RA-5	Minacce, vulnerabilità, probabilità e impatti vengono utilizzati per determinare il rischio	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.SC-4	I fornitori e i partner terzi vengono regolarmente valutati mediante audit, risultati di test o altre forme di valutazio ne per verificare il rispetto degli obblighi contrattuali.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
ID.SC-4	I fornitori e i partner terzi vengono regolarmente valutati mediante audit, risultati di test o altre forme di valutazio ne per verificare il rispetto degli obblighi contrattuali.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.SC-4	I fornitori e i partner terzi vengono regolarmente valutati mediante audit, risultati di test o altre forme di valutazione per verificare il rispetto degli obblighi contrattuali.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.SC-4	I fornitori e i partner terzi vengono regolarmente valutati mediante audit, risultati di test o altre forme di valutazio ne per verificare il rispetto degli obblighi contrattuali.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per dispositivi, utenti e processi autorizzati	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
PR.AC-3	Viene gestito l'accesso remoto.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-3	Viene gestito l'accesso remoto.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-3	Viene gestito l'accesso remoto.	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-3	Viene gestito l'accesso remoto.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
PR.AC-3	Viene gestito l'accesso remoto.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.AC-3	Viene gestito l'accesso remoto.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-3	Viene gestito l'accesso remoto.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete)	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-6	Le identità vengono verificate, legate a credenziali e affermate nelle interazioni	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-6	Le identità vengono verificate, legate a credenziali e affermate nelle interazioni	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-7	Gli utenti, i dispositivi e gli altri asset sono autenticati (ad esempio, a fattore singolo, a più fattori) in base al rischio della transazione (ad esempio, i rischi per la sicurezza e la privacy delle persone e altri rischi organizzativi)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundatio

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			nal Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-7	Gli utenti, i dispositivi e gli altri asset sono autenticati (ad esempio, a fattore singolo, a più fattori) in base al rischio della transazione (ad esempio, i rischi per la sicurezza e la privacy delle persone e altri rischi organizzativi)	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud AWS . Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-7	Gli utenti, i dispositivi e gli altri asset vengono autenticati (ad esempio, a fattore singolo o a più fattori) in base al rischio della transazione (ad esempio, i rischi per la sicurezza e la privacy degli individui e altri rischi organizzativi)	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-7	Gli utenti, i dispositivi e le altre risorse sono autenticati (ad esempio, a fattore singolo, a più fattori) in base al rischio della transazione (ad esempio, i rischi per la sicurezza e la privacy delle persone e altri rischi organizzativi)	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-7	Gli utenti, i dispositivi e gli altri asset vengono autenticati (ad esempio, a fattore singolo o a più fattori) in base al rischio della transazione (ad esempio, i rischi per la sicurezza e la privacy delle persone e altri rischi organizzativi)	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
PR.AT-1	Tutti gli utenti vengono informati e formati	security-awareness-program-exists (controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
PR.DS-1	D ata-at-rest è protetto	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
PR.DS-1	D ata-at-rest è protetto	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
PR.DS-1	D è protetto ata-at-re st	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
PR.DS-1	D ata-at-rest è protetto	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
PR.DS-1	D ata-at-rest è protetto	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
PR.DS-1	D ata-at-rest è protetto	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie in AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D è protetto ata-at-rest	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
PR.DS-1	D ata-at-rest è protetto	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D è protetto ata-at-rest	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
PR.DS-1	D è protetto ata-at-rest	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-1	D ata-at-rest è protetto	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
PR.DS-1	D ata-at-rest è protetto	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-2	D ata-in-transit è protetto	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-2	D è protetto ata-in-transit	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
PR.DS-2	D è protetto ata-in-transit	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-2	D ata-in-transit è protetto	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
PR.DS-2	D è protetto ata-in-transit	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-2	D ata-in-transit è protetto	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
PR.DS-2	D ata-in-transit è protetto	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-2	D è protetto ata-in-transit	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
PR.DS-2	D ata-in-transit è protetto	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-3	Le risorse vengono gestite formalmente durante la rimozione, il trasferimento e la disposizione	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-3	Le risorse vengono gestite formalmente durante la rimozione, il trasferimento e la disposizione	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-3	Le risorse vengono gestite formalmente durante la rimozione , il trasferimento e la disposizione	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibi lità	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibi lità	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibi lità	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibi lità	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibi lità	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibi lità	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibilità	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibi lità	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibilità	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibilità	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibilità	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibilità	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibilità	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibilità	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibi lità	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibi lità	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-4	Viene mantenuta capacità adeguata per garantire la disponibilità	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autorizzazione all'accesso ai repository Bitbucket. GitHub
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
PR.DS-5	Vengono implementate protezioni contro le fughe di dati	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-6	I meccanismi di controllo dell'integrità vengono utilizzati per verificare l'integrità del software, del firmware e delle informazioni	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-6	I meccanismi di controllo dell'integrità vengono utilizzati per verificare l'integrità del software, del firmware e delle informazioni	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-7	L'ambiente o gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-7	L'ambiente o gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-7	L'ambiente o gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-7	L'ambiente o gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-7	L'ambiente o gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-7	L'ambiente o gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione e dei sistemi di controllo industriale che incorpora principi di sicurezza (ad esempio il concetto di minima funzionalità)	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione e dei sistemi di controllo industriale che incorpora i principi di sicurezza (ad esempio il concetto di minima funzionalità)	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione e dei sistemi di controllo industriale che incorpora principi di sicurezza (ad esempio il concetto di minima funzionalità)	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione e dei sistemi di controllo industriale che incorpora principi di sicurezza (ad esempio il concetto di minima funzionalità)	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione e dei sistemi di controllo industriale che incorpora principi di sicurezza (ad esempio il concetto di funzionalità minima)	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione e dei sistemi di controllo industriale che incorpora principi di sicurezza (ad esempio il concetto di funzionalità minima)	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-2	Viene implementato un ciclo di vita di sviluppo del sistema per gestire il sistema	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-2	Viene implement ato un ciclo di vita di sviluppo del sistema per gestire il sistema	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-2	Viene implementato un ciclo di vita di sviluppo del sistema per gestire il sistema	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-3	I processi di controllo delle modifiche alla configurazione sono predisposti	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-3	I processi di controllo delle modifiche alla configurazione sono predisposti	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sat: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-4	I backup delle informazioni vengono eseguiti, gestiti e testati	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-7	I processi di protezione vengono migliorati	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
PR.IP-8	Viene condivisa l'efficacia delle tecnologie di protezione	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-12	Viene sviluppato e implementato un piano di gestione delle vulnerabilità	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-12	Viene sviluppato e implementato un piano di gestione delle vulnerabilità	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee guida per livelli di patch del sistema operativo, installazioni software, configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.IP-12	Viene sviluppato e implementato un piano di gestione delle vulnerabilità	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.MA-2	La manutenzione remota delle risorse dell'organizzazione viene approvata, registrata ed eseguita in modo da impedire l'accesso non autorizzato	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.MA-2	La manutenzione remota delle risorse dell'organizzazione viene approvata, registrata ed eseguita in modo da impedire l'accesso non autorizzato	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni della console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	Le reti di comunicazione e controllo sono protette	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno dell'ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono le informazioni degli account AWS che hanno effettuato l'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-1	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzional ità viene incorpora to configurando i sistemi in modo da fornire solo funzional ità essenziali	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'inter no del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzional ità viene incorpora to configurando i sistemi in modo da fornire solo funzional ità essenziali	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
PR.PT-4	Le reti di comunicazione e controllo sono protette	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	acm-certificate-expiration-check	Assicurati che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
PR.PT-4	Le reti di comunicazione e controllo sono protette	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-4	Le reti di comunicazione e controllo sono protette	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-4	Le reti di comunicazione e controllo sono protette	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-4	Le reti di comunicazione e controllo sono protette	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.PT-4	Le reti di comunicazione e controllo sono protette	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
PR.PT-4	Le reti di comunicazione e controllo sono protette	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-4	Le reti di comunicazione e controllo sono protette	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-5	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RC.RP-1	Il piano di ripristino viene eseguito durante o dopo un incidente di cibersicurezza	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.AN-2	L'impatto dell'incidente viene compreso	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.MI-3	Le vulnerabilità appena identificate vengono mitigate o documentate come rischi accettati	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
RS.RP-1	Viene eseguito il piano di risposta durante o dopo un incidente	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NIST CSF.

Best practice operative per NIST Privacy Framework v1.0

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il NIST Privacy Framework e le regole AWS Config gestite. Ogni AWS Config regola si applica a una AWS risorsa specifica e si riferisce a uno o più controlli del NIST Privacy Framework. Un controllo del NIST Privacy Framework può essere correlato a più regole. AWS Config Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P7	Vengono stabiliti e predisposti i meccanismi per la trasmissione delle autorizzazioni di elaborazione e dei relativi valori dei dati con gli elementi di dati.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
CT.DM-P7	Vengono stabiliti e predisposti i meccanismi per la trasmissione delle autorizzazioni di elaborazione e dei	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativi valori dei dati con gli elementi di dati.		sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
CT.DM-P7	Vengono stabiliti e predisposti i meccanismi per la trasmissione delle autorizzazioni di elaborazione e dei relativi valori dei dati con gli elementi di dati.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P7	Vengono stabiliti e predisposti i meccanismi per la trasmissione delle autorizzazioni di elaborazione e dei relativi valori dei dati con gli elementi di dati.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P7	Vengono stabiliti e predisposti i meccanismi per la trasmissione delle autorizzazioni di elaborazione e dei relativi valori dei dati con gli elementi di dati.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
CT.DM-P7	Vengono stabiliti e predisposti i meccanismi per la trasmissione delle autorizzazioni di elaborazione e dei relativi valori dei dati con gli elementi di dati.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P7	Vengono stabiliti e predisposti i meccanismi per la trasmissione delle autorizzazioni di elaborazione e dei relativi valori dei dati con gli elementi di dati.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
CT.DM-P7	Vengono stabiliti e predisposti i meccanismi per la trasmissione delle autorizzazioni di elaborazione e dei relativi valori dei dati con gli elementi di dati.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P7	Vengono stabiliti e predisposti i meccanismi per la trasmissione delle autorizzazioni di elaborazione e dei relativi valori dei dati con gli elementi di dati.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	audit-log-policy-exists(controllo di processo)	Definizione e mantenimento di una policy di gestione dei log di audit che definisca i requisiti di gestione dei log dell'organizzazione. Ciò include, a titolo esemplificativo, la revisione e la conservazione dei log di audit.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
CT.DM-P8	I record di audit/log vengono determinati, documentati, implementati e rivisti in conformità alla policy e incorporano il principio di riduzione al minimo dei dati.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
ID.DE-P2	Le parti dell'ecosistema di elaborazione dei dati (ad esempio fornitori di servizi, clienti, partner, produttori di prodotti, sviluppatori di applicazioni) vengono identificate, assegnate priorità e valutate utilizzando un processo di valutazione del rischio relativo alla privacy.	annual-risk-assessment-performed(controllo di processo)	Esegui una valutazione annuale del rischio sulla tua organizzazione. Le valutazioni del rischio possono aiutare a determinare la probabilità e l'impatto dei rischi e/o delle vulnerabilità identificati che interessano un'organizzazione.
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
PR.AC-P1	Le identità e le credenziali vengono emesse, gestite, verificate, revocate e sottoposte a audit per utenti, processi e dispositivi autorizzati.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-P3	Viene gestito l'accesso remoto.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
PR.AC-P3	Viene gestito l'accesso remoto.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-P3	Viene gestito l'accesso remoto.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
PR.AC-P3	Viene gestito l'accesso remoto.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.AC-P3	Viene gestito l'accesso remoto.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
PR.AC-P3	Viene gestito l'accesso remoto.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P3	Viene gestito l'accesso remoto.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
PR.AC-P4	I permessi e le autorizzazioni di accesso sono gestiti incorporando i principi del privilegio minimo e della separazione dei compiti.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	acm-certificate-expiration-check	Garantisci che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	ec2-instance-no-pu blic-ip	Gestisci l'accesso al AWS cloud assicuran do che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repositor y di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzional ità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per protegger e il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P5	L'integrità della rete è protetta (ad esempio, segregazione della rete, segmentazione della rete).	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P6	Le persone e i dispositivi sono protetti e vincolati alle credenziali e autenticati in base al rischio della transazione (ad esempio, i rischi per la sicurezza e la privacy delle persone e altri rischi organizzativi).	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundatio

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			nal Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P6	Le persone e i dispositivi sono protetti e vincolati alle credenziali e autentica ti in base al rischio della transazione (ad esempio, i rischi per la sicurezza e la privacy degli individui e altri rischi organizzativi).	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel Cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P6	Le persone e i dispositivi sono protetti e vincolati alle credenziali e autenticati in base al rischio della transazione (ad esempio, i rischi per la sicurezza e la privacy degli individui e altri rischi organizzativi).	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P6	Le persone e i dispositivi sono protetti e vincolati alle credenziali e autenticati in base al rischio della transazione (ad esempio, i rischi per la sicurezza e la privacy degli individui e altri rischi organizzativi).	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.AC-P6	Le persone e i dispositivi sono protetti e vincolati alle credenziali e autenticati in base al rischio della transazione (ad esempio, i rischi per la sicurezza e la privacy delle persone e altri rischi organizzativi).	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
PR.DS-P1	D sono protetti. ata-at-rest	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P1	D ata-at-rest sono protetti.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verifican do l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
PR.DS-P1	D ata-at-rest sono protetti.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P1	D ata-at-rest sono protetti.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
PR.DS-P1	D ata-at-rest sono protetti.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
PR.DS-P1	D ata-at-rest sono protetti.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P1	D ata-at-rest sono protetti.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
PR.DS-P1	D ata-at-rest sono protetti.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P1	D ata-at-rest sono protetti.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
PR.DS-P1	D ata-at-rest sono protetti.	rds-snapshot-encry pted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P1	D ata-at-rest sono protetti.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P1	D ata-at-rest sono protetti.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P1	D sono protetti. ata-at-rest	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.
PR.DS-P1	D ata-at-rest sono protetti.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P1	D ata-at-rest sono protetti.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.
PR.DS-P1	D ata-at-rest sono protetti.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P1	D ata-at-rest sono protetti.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P1	D ata-at-rest sono protetti.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P1	D ata-at-rest sono protetti.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
PR.DS-P2	D sono protetti. ata-in-transit	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P2	D ata-in-transit sono protetti.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
PR.DS-P2	D ata-in-transit sono protetti.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P2	D sono protetti. ata-in-transit	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
PR.DS-P2	D ata-in-transit sono protetti.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibi lità.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibi lità.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibi lità.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviaz ione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfar e i requisiti di resilienz a.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibi lità.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibi lità.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibi lità.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibi lità.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibi lità.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibi lità.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibi lità.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperar e e ripristinare qualsiasi versione di ogni oggetto archiviat o nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzion ali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibi lità.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibi lità.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P4	Viene mantenuta capacità adeguata per garantire la disponibilità.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	dms-replication-not-public	Gestisci l'accesso al cloud assicurando che AWS le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
PR.DS-P5	Vengono implementate protezioni contro le fughe di dati.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.DS-P6	I meccanismi di controllo dell'integrità vengono utilizzati per verificare l'integrità del software, del firmware e delle informazioni.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
PR.MA-P2	La manutenzione remota delle risorse dell'organizzazione e viene approvata, registrata ed eseguita in modo da impedire l'accesso non autorizzato.	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.MA-P2	La manutenzione remota delle risorse dell'organizzazione viene approvata, registrata ed eseguita in modo da impedire l'accesso non autorizzato.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione che incorpora principi di sicurezza (ad esempio, il concetto di minima funzionalità).	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione che incorpora principi di sicurezza (ad esempio, il concetto di funzionalità minima).	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione che incorpora principi di sicurezza (ad esempio, il concetto di minima funzionalità).	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P1	Viene creata e mantenuta una configurazione di base della tecnologi a dell'informazione che incorpora principi di sicurezza (ad esempio, il concetto di minima funzionalità).	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione che incorpora principi di sicurezza (ad esempio, il concetto di minima funzionalità).	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione che incorpora principi di sicurezza (ad esempio, il concetto di minima funzionalità).	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione che incorpora principi di sicurezza (ad esempio, il concetto di minima funzionalità).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P1	Viene creata e mantenuta una configurazione di base della tecnologia dell'informazione che incorpora principi di sicurezza (ad esempio, il concetto di minima funzionalità).	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
AT-1: PR.PO-P10	Viene sviluppato e implementato un piano di gestione delle vulnerabilità.	vuln-management-plan-exists(controllo di processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P2	Vengono stabiliti e predisposti i processi di controllo delle modifiche alla configurazione.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P2	Vengono stabiliti e predisposti i processi di controllo delle modifiche alla configurazione.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P3	I backup delle informazioni vengono eseguiti, gestiti e testati.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuit à aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristin o di emergenza) vengono stabiliti, predisposti e gestiti.	backup-recovery-po int-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuit à aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristin o di emergenza) vengono stabiliti, predisposti e gestiti.	backup-recovery-po int-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PO-P7	I piani di risposta (Risposta agli eventi imprevisti e Continuità aziendale) e i piani di ripristino (Ripristino da un incidente e Ripristino di emergenza) vengono stabiliti, predisposti e gestiti.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
PR.PO-P8	I piani di risposta e ripristino vengono testati.	response-plan-tested(controllo di processo)	Verifica che i piani di risposta agli incidenti e di ripristino siano testati. Questo può aiutare a capire se il piano sarà efficace in caso di incidente e se è necessario risolvere eventuali lacune o apportare aggiornamenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzional ità viene incorpora to configurando i sistemi in modo da fornire solo funzional ità essenziali.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P2	Il principio della minima funzionalità viene incorporato configurando i sistemi in modo da fornire solo funzionalità essenziali.	redshift-enhanced-vpc-routing-enabled	Il routing VPC avanzato forza tutto il traffico COPY e UNLOAD tra il cluster e i repository di dati a passare attraverso Amazon VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare i log di flusso VPC per monitorare il traffico di rete.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	acm-certificate-expiration-check	Garantisci che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P3	Le reti di comunicazione e controllo sono protette.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
PR.PT-P4	Vengono implement ati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
PR.PT-P4	Vengono implement ati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
PR.PT-P4	Vengono implementati meccanismi (ad esempio failsafe, load balancing, hot swap) per soddisfare i requisiti di resilienza in situazioni normali e avverse.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NIST Privacy Framework v1.0.

Best practice operative per NYDFS 23

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra i requisiti di sicurezza informatica del Dipartimento dei Servizi Finanziari dello Stato di New York (NYDFS) per le società di servizi finanziari (23 NYCRR 500) e le regole di Config gestite. AWS Ogni AWS Config regola si applica a una AWS risorsa specifica e si riferisce a uno o più controlli del NYDFS degli Stati Uniti. Un controllo US NYDFS 23 NYCRR 500 può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.		possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché nell' SageMaker endpoint possono esistere dati sensibili inattivi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportano il mantenimento di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciamento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimensionamento automatico. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(a)	(a) Programma di cibersicurezza. Ogni entità coperta deve mantenere un programma di cibersicurezza concepito per proteggere la riservatezza, l'integrità e la disponibilità dei suoi sistemi informativi.	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per proteggere l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	s3-bucket-public-w rite-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibi lità, compromet tere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (2) utilizzare un'infras truttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazi oni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizion i di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(2)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (2) utilizzare un'infrastruttura difensiva e attuare policy e procedure per proteggere i sistemi informativi dell'entità coperta e le informazioni non pubbliche archiviate in tali sistemi da accessi e usi non autorizzati o altri atti dannosi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorar e la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(3)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (3) rilevare gli eventi di cibersicurezza.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (5) eseguire il ripristino in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (5) eseguire il ripristino in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (5) eseguire il ripristino in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (5) eseguire il ripristino in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (5) eseguire il ripristin o in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (5) eseguire il ripristino in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondamentali di cibersicurezza: (5) eseguire il ripristino in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (5) eseguire il ripristin o in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (5) eseguire il ripristin o in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (5) eseguire il ripristin o in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (5) eseguire il ripristin o in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (5) eseguire il ripristin o in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	backup-plan-min-fr equency-and-min-re tention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservaz ione minime. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredF requencyValue (Config default: 1), (requiredRetentionD ays Config default: 35) e (requiredF requencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
500.02(b)(5)	(b) Il programma di cibersicurezza deve essere basato sulla valutazione del rischio dell'entità coperta e concepito per svolgere le seguenti funzioni fondament ali di cibersicurezza: (5) eseguire il ripristin o in seguito a eventi di cibersicurezza e riprendere le operazioni e i servizi consueti.	backup-recovery-po int-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,05	Il programma di cibersicurezza per ciascuna entità coperta deve includere monitoraggio e test sviluppati in conformità alla valutazione del rischio dell'entità coperta e concepiti per valutare l'efficacia del relativo programma di cibersicurezza. Il monitoraggio e i test devono includere il monitoraggio continuo o test di penetrazione e valutazioni delle vulnerabilità periodici. In assenza di un monitoraggio continuo efficace o di altri sistemi per rilevare, su base continuativa, le modifiche nei sistemi informativi che possono creare o indicare vulnerabilità, le entità coperte devono condurre: (a) test di penetrazione annuali dei sistemi informativi dell'enti	vuln-management-plan-exists (controllo del processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	tà coperta, stabiliti ogni anno sulla base dei rischi rilevanti identificati in conformità alla valutazione del rischio e (b) valutazioni biennali delle vulnerabilità, tra cui eventuali scansioni o revisioni sistematiche dei sistemi informativi ragionevolmente concepite per identificare vulnerabilità di cibersicurezza pubblicamente note nei sistemi informativi dell'entità coperta in base alla valutazione del rischio.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazio ne del rischio: (1) sono concepiti per ricostruire le transazio ni finanziarie rilevanti sufficienti a supportar e le normali operazion i e gli obblighi dell'enti tà coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabili tà di danneggia re materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(b)	(b) Ciascuna entità coperta deve conservare i record richiesti nella sezione 500.06(a)(1) della presente parte per almeno cinque anni e deve conservare i record richiesti nella sezione 500.06(a)(2) della presente parte per almeno tre anni.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.06(a)	(a) Ciascuna entità coperta deve mantenere in sicurezza i sistemi che, nella misura applicabile e sulla base della valutazione del rischio: (1) sono concepiti per ricostruire le transazioni finanziarie rilevanti sufficienti a supportare le normali operazioni e gli obblighi dell'entità coperta e (2) includono audit trail pensati per rilevare e affrontare gli eventi di cibersicurezza che hanno una ragionevole probabilità di danneggiare materialmente qualsiasi parte materiale delle normali operazioni dell'entità coperta.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	ecs-task-definition-user-for-host-mode-check	Se una definizione di attività ha privilegi elevati, significa che il cliente ha scelto specificamente di accedere a tali configurazioni. Questo controllo verifica l'aumento imprevisto dei privilegi quando la rete host prevede una definizione di attività ma il cliente non ha scelto privilegi elevati.
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia di password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del Cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
500,07	Nell'ambito del suo programma di cibersicurezza, sulla base della valutazione del rischio dell'entità coperta, ogni entità coperta limiterà i privilegi di accesso degli utenti ai sistemi informativi che forniscono accesso a informazioni non pubbliche e rivedrà periodicamente tali privilegi.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.8(a)	(a) Il programma di cibersicurezza di ciascuna entità coperta deve includere procedure , linee guida e standard scritti concepiti per garantire l'uso di pratiche di sviluppo sicure per le applicazioni sviluppat e internamente e utilizzate dall'entità coperta e procedure per valutare o testare la sicurezza delle applicazioni sviluppat e esternamente e utilizzate dall'entità coperta nel contesto del suo ambiente tecnologico.	codebuild-project-envvar-awscred-check	Assicurati che le credenziali di autenticazione AWS_ACCES S_KEY_ID e AWS_SECRE T_ACCESS_KEY non esistano negli ambienti del progetto Codebuild. AWS Non archiviare queste variabili con testo in chiaro. L'archiviazione di queste variabili con testo in chiaro porta all'esposizione involontaria dei dati e all'accesso non autorizzato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.8(a)	(a) Il programma di cibersicurezza di ciascuna entità coperta deve includere procedure , linee guida e standard scritti concepiti per garantire l'uso di pratiche di sviluppo sicure per le applicazioni sviluppat e internamente e utilizzate dall'entità coperta e procedure per valutare o testare la sicurezza delle applicazioni sviluppat e esternamente e utilizzate dall'entità coperta nel contesto del suo ambiente tecnologico.	codebuild-project-source-repo-url-check	Assicurati che l'URL del repository di origine GitHub o Bitbucket non contenga token di accesso personali e credenziali di accesso all'interno degli ambienti del progetto Codebuild. AWS Utilizza OAuth anziché i token di accesso personali o le credenziali di accesso per concedere l'autoriz zazione all'accesso ai repository Bitbucket. GitHub

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,09	(a) Ciascuna entità coperta deve condurre una valutazione periodica del rischio dei suoi sistemi informativi sufficiente a orientare la progettazione del programma di cibersicurezza, come richiesto nella presente parte. Tale valutazione del rischio deve essere aggiornata se ragionevolmente necessario per affrontare le modifiche ai sistemi informativi, alle informazioni non pubbliche o alle operazioni commerciali dell'entità coperta. La valutazione del rischio dell'entità coperta deve fare in modo che la revisione dei controlli risponda agli sviluppi tecnologici e alle minacce in evoluzione e tenere conto dei rischi particolari delle operazioni	annual-risk-assessment-performed (controllo del processo) >	Esegui una valutazione annuale del rischio sulla tua organizzazione. Le valutazioni del rischio possono aiutare a determinare la probabilità e l'impatto dei rischi e/o delle vulnerabilità identificati che interessano un'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	commerciali dell'entità coperta relativi alla cibersicurezza, alle informazioni non pubbliche raccolte o archiviate, ai sistemi informativi utilizzati e alla disponibilità e all'efficacia dei controlli per proteggere le informazioni non pubbliche e i sistemi informativi.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,12	(a) Autenticazione a più fattori. Sulla base della valutazione del rischio, ogni entità coperta deve utilizzare controlli efficaci, che possono includere l'autenticazione a più fattori o l'autenticazione basata sul rischio, per proteggersi dall'accesso non autorizzato a informazioni non pubbliche o sistemi informativi. (b) L'autenticazione a più fattori deve essere utilizzata per qualsiasi persona che accede alle reti interne dell'entità coperta da una rete esterna, a meno che il CISO dell'entità coperta non abbia approvato per iscritto l'uso di controlli di accesso ragionevolmente equivalenti o più sicuri.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS Cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.12	(a) Autenticazione a più fattori. Sulla base della valutazione del rischio, ogni entità coperta deve utilizzare controlli efficaci, che possono includere l'autenticazione a più fattori o l'autenticazione basata sul rischio, per proteggersi dall'accesso non autorizzato a informazioni non pubbliche o sistemi informativi. (b) L'autenticazione a più fattori deve essere utilizzata per qualsiasi persona che accede alle reti interne dell'entità coperta da una rete esterna, a meno che il CISO dell'entità coperta non abbia approvato per iscritto l'uso di controlli di accesso ragionevolmente equivalenti o più sicuri.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,12	(a) Autenticazione a più fattori. Sulla base della valutazione del rischio, ogni entità coperta deve utilizzare controlli efficaci, che possono includere l'autenticazione a più fattori o l'autenticazione basata sul rischio, per proteggersi dall'accesso non autorizzato a informazioni non pubbliche o sistemi informativi. (b) L'autenticazione a più fattori deve essere utilizzata per qualsiasi persona che accede alle reti interne dell'entità coperta da una rete esterna, a meno che il CISO dell'entità coperta non abbia approvato per iscritto l'uso di controlli di accesso ragionevolmente equivalenti o più sicuri.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,12	(a) Autenticazione a più fattori. Sulla base della valutazione del rischio, ogni entità coperta deve utilizzare controlli efficaci, che possono includere l'autenticazione a più fattori o l'autenticazione basata sul rischio, per proteggersi dall'accesso non autorizzato a informazioni non pubbliche o sistemi informativi. (b) L'autenticazione a più fattori deve essere utilizzata per qualsiasi persona che accede alle reti interne dell'entità coperta da una rete esterna, a meno che il CISO dell'entità coperta non abbia approvato per iscritto l'uso di controlli di accesso ragionevolmente equivalenti o più sicuri.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,12	(a) Autenticazione a più fattori. Sulla base della valutazione del rischio, ogni entità coperta deve utilizzare controlli efficaci, che possono includere l'autenticazione a più fattori o l'autenticazione basata sul rischio, per proteggersi dall'accesso non autorizzato a informazioni non pubbliche o sistemi informativi. (b) L'autenticazione a più fattori deve essere utilizzata per qualsiasi persona che accede alle reti interne dell'entità coperta da una rete esterna, a meno che il CISO dell'entità coperta non abbia approvato per iscritto l'uso di controlli di accesso ragionevolmente equivalenti o più sicuri.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	cloudwatch-alarm-action-check	Amazon avvisa CloudWatch quando una metrica supera la soglia per un determinato numero di periodi di valutazione. L'allarme esegue una o più operazioni basate sul valore del parametro o espressione relativa a una soglia su un certo numero di periodi. Questa regola richiede un valore per alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), (okActionRequired Config Default: False). Il valore effettivo deve riflettere le operazioni di allarme per il tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) su ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.14(a)	(a) implementa policy, procedure e controlli basati sul rischio concepiti per monitorare l'attività degli utenti autorizzati e rilevare l'accesso o l'uso non autorizzato o la manomissione di informazioni non pubbliche da parte di questi utenti autorizzati.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
500.14(b)	Nell'ambito del programma di cibersicurezza, ogni entità coperta deve: (b) fornire a tutto il personale una formazione periodica di sensibilizzazione alla cibersicurezza, aggiornata in base ai rischi identificati dall'entità coperta nella valutazione del rischio.	security-awareness-program-exists (controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli, inclusa la crittografia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittografia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli, inclusa la crittografia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	api-gw-cache-enabl ed-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per protegger e i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	elasticsearch-encr ypted-at-rest	Poiché possono esistere dati sensibili e per protegger e i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli, inclusa la crittografia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittografia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittografia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	s3-bucket-ssl-requ ests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizz o di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	sagemaker-endpoint -configuration-kms- key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	sagemaker-notebook -instance-kms-key- configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurat i che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittogra fia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli, inclusa la crittografia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli, inclusa la crittografia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittogra fia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	dynamodb-table-enc rypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazi one predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviat i, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.
500.15(a)	(a) Nell'ambito del programma di cibersicurezza, sulla base della valutazione del rischio, ciascuna entità coperta deve implementare controlli , inclusa la crittogra fia, per proteggere le informazioni non pubbliche detenute o trasmesse dall'entità coperta sia in transito su reti esterne sia a riposo.	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
500,16	(a) Nell'ambito del programma di cibersicurezza, ciascuna entità coperta deve stabilire un piano scritto di risposta agli incidenti concepito per affrontare tempestiv amente ed eseguire il ripristino da qualsiasi evento di cibersicu rezza che influisca materialmente sulla riservatezza, sull'inte grità o sulla disponibi lità dei sistemi informativi dell'enti tà coperta o sulla continua funzionalità di qualsiasi aspetto dell'attività o delle operazioni dell'entità coperta.	response-plan-exists-maintained (controllo del processo)	Garanzia della definizione, del mantenimento e della distribuzione al personale responsab ile di piani di risposta agli incidenti.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NYDFS 23.

Best practice operative per NZISM

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti

di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il Manuale sulla sicurezza delle informazioni (NZISM) 2022-09 versione 3.6 del New Zealand Government Communications Security Bureau (GCSB) e le regole di Managed Config. AWS Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli NZISM. Un controllo NZISM può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

Questo modello di pacchetto di conformità di esempio contiene mappature ai controlli all'interno del framework NZISM, parte integrante del framework Protective Security Requirements (PSR) che definisce le aspettative del governo neozelandese relativamente alla gestione del personale, delle informazioni e della sicurezza fisica.

Il framework NZISM viene concesso tramite licenza Creative Commons Attribution 4.0 New Zealand, disponibile all'indirizzo https://creativecommons.org/licenses/by/4.0/. Per informazioni sul copyright, consulta NZISM New Zealand Information Security Manual | Legal, Privacy, and Copyright.

ID controllo	AWS Regola di configurazione	Linea guida
1149	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
1149	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.
1149	ecs-containers-nonprivileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).

ID controllo	AWS Regola di configurazione	Linea guida
1149	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
1149	ec2- hardening-and-state-management (Controllo del processo)	I processi avanzati di creazione delle immagini del server EC2 e le associazioni State Manager sono configurati in modo da rimuovere componenti e servizi non necessari e installare software antimalware e agenti di log.

ID controllo	AWS Regola di configurazione	Linea guida
1661	cloudfront-default-root-object-configured	Questo controllo verifica se una CloudFront distribuzione Amazon è configurata per restituire un oggetto specifico che è l'oggetto root predefini to. Il controllo fallisce se nella CloudFront distribuzione non è configurato un oggetto root predefinito. A volte un utente può richiedere l'URL principal e della distribuzione anziché un oggetto nella distribuz ione. In tal caso, la specifica di un oggetto root predefini to può contribuire a evitare l'esposizione dei contenuti della distribuzione Web. Questa regola deve essere applicata nella regione us-east-1.
1667	acm-certificate-expiration-check	Garantisci la protezion e dell'integrità della rete assicurando che i certifica ti X509 vengano emessi da ACM. AWS Questi certifica ti devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
1667	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
1841	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
1841	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
1841	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
1841	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
1847	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittogra fate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
1847	cloudfront-viewer-policy-https	Questo controllo verifica se una CloudFront distribuzione Amazon richiede agli spettatori di utilizzare direttamente HTTPS o se utilizza il reindirizzamento. Il controllo ha esito negativo se ViewerProtocolPolicy è impostato su allow-all per o per CacheBehaviors defaultCacheBehavior . HTTPS (TLS) può essere utilizzato per impedire a potenziali aggressori di utilizzare o attacchi simili per intercettare person-in-the-middle o manipolare il traffico di rete. Devono essere consentite solo le connessioni crittografate tramite HTTPS (TLS). Questa regola deve essere applicata nella regione us-east-1.

ID controllo	AWS Regola di configurazione	Linea guida
1847	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
1847	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
1847	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
1858	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti stabiliti dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
1893	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzat e per un periodo di tempo specificato. Se rilevi credenzia li inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsage Age (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'orga nizzazione.
1893	federate-with-central-idp (Controllo del processo)	Le identità della forza lavoro che richiedono l'accesso alle AWS risorse vengono autenticate con un IdP centrale federato con SSO. AWS L'IdP centrale blocca gli utenti del sistema dopo 3 tentativi di accesso falliti.

ID controllo	AWS Regola di configurazione	Linea guida
1946	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
1946	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di configurazione	Linea guida
1998	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
1998	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
1998	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.
2013	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
2013	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
2013	cloudfront-accesslogs-enabled	Questo controllo verifica se la registrazione degli accessi al server è abilitata sulle CloudFront distribuzioni. Il controllo ha esito negativo se la registrazione dei log di accesso non è abilitata per una distribuzione. CloudFront i registri di accesso forniscon o informazioni dettagliate su ogni richiesta utente ricevuta. CloudFront Ogni log contiene informazioni come la data e l'ora di ricezione della richiesta, l'indirizzo IP del visualizzatore che ha effettuat o la richiesta, l'origine della richiesta e il numero di porta della richiesta del visualizz atore. Questi log sono utili per applicazioni quali audit di sicurezza e accesso e indagini forensi. Questa regola deve essere applicata nella regione us-east-1.

ID controllo	AWS Regola di configurazione	Linea guida
2013	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
2013	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	AWS Regola di configurazione	Linea guida
2013	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di configurazione	Linea guida
2022	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
2022	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	AWS Regola di configurazione	Linea guida
2028	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.
2082	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo. È disponibile un'esenzione per gli ambienti di preproduzione.
2082	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
2082	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
2082	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
2082	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
2082	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	AWS Regola di configurazione	Linea guida
2082	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
2082	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
2082	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
2082	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
2082	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
2091	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
2091	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
2091	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedan o la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
2598	elb-custom-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che i tuoi listener ElasticLoadBalancer SSL Classic utilizzino una politica di sicurezza personalizzata. Queste policy possono fornire diversi algoritmi crittografici ad alta resistenza per contribuire a garantire comunicazioni di rete crittografate tra i sistemi. Questa regola richiede l'impostazione di una policy di sicurezza personalizzata per gli ascoltatori SSL. La politica di sicurezza predefinita è: Protocol-TLSv1.2,ECDHE-ECDSA-AES128-GCM-SHA256.

ID controllo	AWS Regola di configurazione	Linea guida
2600	elb-custom-security-policy-ssl-check	Per proteggere i dati in transito, assicurati che i tuoi listener ElasticLoadBalancer SSL Classic utilizzino una politica di sicurezza personalizzata. Queste policy possono fornire diversi algoritmi crittografici ad alta resistenza per contribuire a garantire comunicazioni di rete crittografate tra i sistemi. Questa regola richiede l'impostazione di una policy di sicurezza personalizzata per gli ascoltatori SSL. La politica di sicurezza predefinita è: Protocol-TLSv1.2,ECDHE-ECDSA-AES128-GCM-SHA256.
2726	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di configurazione	Linea guida
3021	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.
3021	kms-cmk- for-each-data-classification (Controllo del processo)	È stata definita almeno una chiave master del cliente (CMK) di KMS per ogni distinta classificazione dei dati e le CMK vengono utilizzat e per crittografare tutti i dati archiviati in quella classific azione.
3205	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di configurazione	Linea guida
3449	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
3449	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilitazione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

ID controllo	AWS Regola di configurazione	Linea guida
3449	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.
3451	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
3451	ec2-critical- security-patch-auto-approval (Controllo del processo)	Le baseline delle patch per Windows e/o Linux sono state configurate in Patch Manager, inclusa l'approva zione automatica delle patch di sicurezza critiche entro 2 giorni dal rilascio.
3452	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
3452	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornam enti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisc e l'installazione degli ultimi aggiornamenti, correzion i e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	AWS Regola di configurazione	Linea guida
3452	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.
3453	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
3453	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
3562	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
3562	cloudfront-associated-with-waf	Questo controllo verifica se CloudFront le distribuzioni sono associate agli ACL Web AWS WAF o AWS WAFv2. Il controllo ha esito negativo se la distribuzione non è associata a un ACL web. AWS WAF è un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web e le API dagli attacchi. Consente di configurare un set di regole denominato lista di controllo degli accessi Web (ACL web) per consentire, bloccare o contare le richieste Web in base a condizioni e regole di sicurezza Web personalizzabili definite dall'utente. Assicurati che la tua CloudFront distribuzione sia associata a un ACL web AWS WAF per proteggerla da attacchi dannosi. Questa regola deve essere applicata nella regione us-east-1.

ID controllo	AWS Regola di configurazione	Linea guida
3562	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicam ente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
3562	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per protegger e l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
3562	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
3562	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
3562	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
3562	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di configurazione	Linea guida
3562	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.
3562	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di configurazione	Linea guida
3562	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
3562	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
3562	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3562	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
3562	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
3562	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS
3562	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	AWS Regola di configurazione	Linea guida
3623	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
3623	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	AWS Regola di configurazione	Linea guida
3623	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3623	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
3815	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	AWS Regola di configurazione	Linea guida
3875	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.
3875	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di configurazione	Linea guida
4333	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.
4441	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
4441	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	AWS Regola di configurazione	Linea guida
4441	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
4441	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
4441	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
4441	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.
4441	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
4445	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
4445	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittogra fia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configura zioni richieste siano implement ate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). I valori effettivi devono rifletter e le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
4829	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).
4829	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata. Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	AWS Regola di configurazione	Linea guida
4829	rds-cluster-multi-az-enabled	Per favorire la disponibilità dei dati archiviati, la replica Multi-AZ deve essere abilitata per i cluster Amazon Relational Database Service (Amazon RDS). Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
4829	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprendere le operazioni del database non appena il failover è completato.

ID controllo	AWS Regola di configurazione	Linea guida
4838	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.
4838	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
4838	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
4838	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Regola di configurazione	Linea guida
4838	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
4839	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
4839	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	AWS Regola di configurazione	Linea guida
4839	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
4839	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
4839	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
4839	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
4839	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
4839	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
4839	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
4839	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
4839	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.
4839	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
4839	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
4839	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.
4839	sagemaker-notebook-instance-kms-key-configured	Per contribuire a proteggere i dati archiviati, assicuratevi che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il notebook SageMaker . Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
4839	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.
4839	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
4849	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
4849	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
4849	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
4849	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
4849	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
4849	elasticache-redis-cluster-a utomatic-backup-check	Quando i backup automatic i sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornalie ra. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazion e. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	AWS Regola di configurazione	Linea guida
4849	rds-cluster-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzion almente, con conseguente perdita di disponibilità delle applicazioni.
4849	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
4849	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relational Database Service (Amazon RDS) sia abilitata la protezione da eliminazione. Utilizza la protezione da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
4849	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	AWS Regola di configurazione	Linea guida
4849	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.
6843	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
6843	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
6852	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
6852	federate-with-central-idp (Controllo del processo)	Le identità della forza lavoro che richiedono l'accesso alle AWS risorse vengono autenticate con un IdP centrale federato con SSO. AWS L'IdP centrale blocca gli utenti del sistema dopo 3 tentativi di accesso falliti.
6860	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
6860	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
6861	cloudtrail-security-trail-enabled	Questa regola aiuta a garantire l'uso delle migliori pratiche di sicurezza AWS consigliate per AWS CloudTrail, verificando l'abilitazione di più impostazioni. Queste includono l'uso della crittografia dei log, la convalida dei log e l'abilitazione AWS CloudTrail in più aree.
6953	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
6953	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
7436	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
7436	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
7436	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
7436	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
7437	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
7437	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.
7437	root-account-hardware-mfa-e nabled	Gestisci l'accesso alle risorse nel AWS cloud assicuran doti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
7437	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenti cazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromis sione. Account AWS
7466	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per protegger e le applicazioni web. Un WAF aiuta a proteggere le applicazi oni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
7466	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicam ente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
7466	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per protegger e l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.
7466	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
7466	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
7466	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
7466	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di configurazione	Linea guida
7466	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS Cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.
7466	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di configurazione	Linea guida
7466	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
7466	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di configurazione	Linea guida
7466	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
7466	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
7466	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
7466	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
7466	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	AWS Regola di configurazione	Linea guida
7466	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
7496	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
7496	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	AWS Regola di configurazione	Linea guida
7496	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrai l Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	AWS Regola di configurazione	Linea guida
7496	cloudfront-accesslogs-enabled	Questo controllo verifica se la registrazione degli accessi al server è abilitata sulle CloudFront distribuzioni. Il controllo ha esito negativo se la registrazione dei log di accesso non è abilitata per una distribuzione. CloudFront i registri di accesso forniscon o informazioni dettagliate su ogni richiesta utente ricevuta. CloudFront Ogni log contiene informazioni come la data e l'ora di ricezione della richiesta, l'indirizzo IP del visualizzatore che ha effettuat o la richiesta, l'origine della richiesta e il numero di porta della richiesta del visualizz atore. Questi log sono utili per applicazioni quali audit di sicurezza e accesso e indagini forensi. Questa regola deve essere applicata nella regione us-east-1.
7496	cloudwatch-log-group-encryp ted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	AWS Regola di configurazione	Linea guida
7496	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registraz ione di log di ELB sia abilitata . I dati raccolti forniscon o informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazi oni come l'ora in cui è stata ricevuta la richiesta, l'indiriz zo IP del client, le latenze, i percorsi delle richieste e le risposte del server.
7496	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	AWS Regola di configurazione	Linea guida
7496	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL Web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for NZISM.

Best practice operative per PCI DSS 3.2.1

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 e le regole Config gestite AWS . Ogni AWS Config regola si applica a una AWS risorsa specifica e si riferisce a uno o più controlli PCI DSS. Un controllo PCI DSS può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	alb-desync-mode-check	Per contribuire a proteggere le applicazioni dalle vulnerabilità della desincronizzazione HTTP, assicurati che la modalità di mitigazione della desincronizzazione HTTP sia abilitata sui sistemi di bilanciamento del carico delle applicazioni. I problemi di desincronizzazione HTTP possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della cache e della coda delle richieste. Le modalità di mitigazione della desincronizzazione sono Monitoraggio, Difensiva e Più rigorosa. Difensiva è la modalità predefinita.
1.2.1	Limita il traffico in entrata e in uscita	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.		(ELB) siano configura ti per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicuran doti che le istantane e EBS non siano ripristinabili pubblicam ente. Gli snapshot dei volumi EBS possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicuran do che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicuran do che i nodi master del cluster Amazon EMR non siano accessibili pubblicam ente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	netfw-stateless-rule-group-not-empty	Un gruppo di regole AWS Network Firewall contiene regole che definiscono il modo in cui il firewall elabora il traffico nel tuo VPC. Un gruppo di regole stateless vuoto, se presente in una policy firewall, non elabora il traffico.
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearc h Service all'inter no di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.2.1	Limita il traffico in entrata e in uscita a quello necessario per l'ambiente dati del titolare della carta e nega specifica mente tutto il restante traffico.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	alb-desync-mode-check	Per contribuire a proteggere le applicazioni dalle vulnerabilità della desincronizzazione HTTP, assicurati che la modalità di mitigazione della desincronizzazione HTTP sia abilitata sui sistemi di bilanciamento del carico delle applicazioni. I problemi di desincronizzazione HTTP possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della cache e della coda delle richieste. Le modalità di mitigazione della desincronizzazione sono Monitoraggio, Difensiva e Più rigorosa. Difensiva è la modalità predefinita.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configura ti per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	netfw-stateless-rule-group-not-empty	Un gruppo di regole AWS Network Firewall contiene regole che definiscono il modo in cui il firewall elabora il traffico nel tuo VPC. Un gruppo di regole stateless vuoto, se presente in una policy firewall, non elabora il traffico.
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3	Proibisci l'accesso pubblico diretto tra Internet e qualsiasi componente di sistema nell'ambiente di dati del titolare della carta.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicamente autorizzati.	alb-desync-mode-check	Per contribuire a proteggere le applicazioni dalle vulnerabilità della desincronizzazione HTTP, assicurati che la modalità di mitigazione della desincronizzazione HTTP sia abilitata sui sistemi di bilanciamento del carico delle applicazioni. I problemi di desincronizzazione HTTP possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della cache e della coda delle richieste. Le modalità di mitigazione della desincronizzazione sono Monitoraggio, Difensiva e Più rigorosa. Difensiva è la modalità predefinita.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configura ti per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibi li pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicuran do che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicamente autorizzati.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicamente autorizzati.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'inter no di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearc h servizio all'inter no di un Amazon VPC consente una comunicazione sicura tra il OpenSearc h Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicamente autorizzati.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicaz ione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'inter no del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicamente autorizzati.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	netfw-stateless-rule-group-not-empty	Un gruppo di regole AWS Network Firewall contiene regole che definiscono il modo in cui il firewall elabora il traffico nel tuo VPC. Un gruppo di regole stateless vuoto, se presente in una policy firewall, non elabora il traffico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicamente autorizzati.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibi lità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPo rt1 - blockedPort5 (valori di configura zione predefiniti: 20,21,3389,3306,43 33). I valori effettivi devono riflettere le policy dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicamente autorizzati.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicamente autorizzati.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicamente autorizzati.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicamente autorizzati.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicamente autorizzati.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.1	Implementa una DMZ per limitare il traffico in ingresso solo ai componenti di sistema che forniscono servizi, protocolli e porte accessibili pubblicam ente autorizzati.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	alb-desync-mode-check	Per contribuire a proteggere le applicazioni dalle vulnerabilità della desincronizzazione HTTP, assicurati che la modalità di mitigazione della desincronizzazione HTTP sia abilitata sui sistemi di bilanciamento del carico delle applicazioni. I problemi di desincronizzazione HTTP possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della cache e della coda delle richieste. Le modalità di mitigazione della desincronizzazione sono Monitoraggio, Difensiva e Più rigorosa. Difensiva è la modalità predefinita.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	netfw-stateless-rule-group-not-empty	Un gruppo di regole AWS Network Firewall contiene regole che definiscono il modo in cui il firewall elabora il traffico nel tuo VPC. Un gruppo di regole stateless vuoto, se presente in una policy firewall, non elabora il traffico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.2	Limita il traffico Internet in ingresso agli indirizzi IP all'interno della DMZ.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	alb-desync-mode-check	Per contribuire a proteggere le applicazioni dalle vulnerabilità della desincronizzazione HTTP, assicurati che la modalità di mitigazione della desincronizzazione HTTP sia abilitata sui sistemi di bilanciamento del carico delle applicazioni. I problemi di desincronizzazione HTTP possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della cache e della coda delle richieste. Le modalità di mitigazione della desincronizzazione sono Monitoraggio, Difensiva e Più rigorosa. Difensiva è la modalità predefinita.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambi ente dati del titolare della carta a Internet.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	netfw-stateless-rule-group-not-empty	Un gruppo di regole AWS Network Firewall contiene regole che definiscono il modo in cui il firewall elabora il traffico nel tuo VPC. Un gruppo di regole stateless vuoto, se presente in una policy firewall, non elabora il traffico.
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambi ente dati del titolare della carta a Internet.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambi ente dati del titolare della carta a Internet.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambi ente dati del titolare della carta a Internet.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.4	Non consentire il traffico in uscita non autorizzato dall'ambiente dati del titolare della carta a Internet.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	netfw-policy-rule-group-associated	Una policy AWS Network Firewall definisce il modo in cui il firewall monitora e gestisce il traffico in un Amazon VPC. Puoi configurare gruppi di regole stateless e stateful per filtrare pacchetti e flussi di traffico, nonché definire la gestione del traffico predefinita.
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	netfw-stateless-rule-group-not-empty	Un gruppo di regole AWS Network Firewall contiene regole che definiscono il modo in cui il firewall elabora il traffico nel tuo VPC. Un gruppo di regole stateless vuoto, se presente in una policy firewall, non elabora il traffico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
1.3.6	Posiziona i componenti di sistema che archiviano i dati del titolare della carta (ad esempio un database) in una zona di rete interna, separata dalla DMZ e da altre reti non attendibili.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1	Modifica sempre le impostazioni predefinite del fornitore e rimuovi o disabilita gli account predefiniti non necessari prima di installare un sistema in rete. Ciò si applica a TUTTE le password predefinite, incluse, a titolo esemplificativo ma non esaustivo, quelle utilizzate dai sistemi operativi, dal software che fornisce servizi di sicurezza, account di applicazioni e di sistema, terminali point-of-sale (POS), applicazioni di pagamento, stringhe di community Simple Network Management Protocol (SNMP), ecc.).	rds-cluster-default-admin-check	Poiché i nomi utente predefiniti sono di dominio pubblico, la loro modifica può aiutare a ridurre la superficie di attacco dei cluster database Amazon Relational Database Service (Amazon RDS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1	Modifica sempre le impostazioni predefinite del fornitore e rimuovi o disabilita gli account predefiniti non necessari prima di installare un sistema in rete. Ciò si applica a TUTTE le password predefinite, incluse, a titolo esemplificativo ma non esaustivo, quelle utilizzate dai sistemi operativi, dal software che fornisce servizi di sicurezza, dagli account di applicazione e di sistema, dai terminali point-of-sale (POS), dalle applicazioni di pagamento, dalle stringhe della community SNMP (Simple Network Management Protocol), ecc.).	rds-instance-default-admin-check	Poiché i nomi utente predefiniti sono di dominio pubblico, la loro modifica può aiutare a ridurre la superficie di attacco per le istanze database Amazon Relational Database Service (Amazon RDS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1	Modifica sempre le impostazioni predefinite del fornitore e rimuovi o disabilita gli account predefiniti non necessari prima di installare un sistema in rete. Ciò si applica a TUTTE le password predefinite, incluse, a titolo esemplificativo ma non esaustivo, quelle utilizzate dai sistemi operativi, dal software che fornisce servizi di sicurezza, dagli account di applicazione e di sistema, dai terminali point-of-sale (POS), dalle applicazioni di pagamento, dalle stringhe della community SNMP (Simple Network Management Protocol), ecc.).	redshift-default-admin-check	Poiché i nomi utente predefiniti sono di dominio pubblico, la loro modifica può aiutare a ridurre la superficie di attacco dei cluster Amazon Redshift.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1	Modifica sempre le impostazioni predefinite del fornitore e rimuovi o disabilita gli account predefiniti non necessari prima di installare un sistema in rete. Ciò si applica a TUTTE le password predefinite, incluse, a titolo esemplificativo ma non esaustivo, quelle utilizzate dai sistemi operativi, dal software che fornisce servizi di sicurezza, dagli account di applicazione e di sistema, dai terminali point-of-sale (POS), dalle applicazioni di pagamento, dalle stringhe della community SNMP (Simple Network Management Protocol), ecc.).	redshift-default-db-name-check	I nomi predefiniti sono di dominio pubblico e devono essere modificati al momento della configurazione. La modifica del nome del database predefinito del cluster Amazon Redshift può aiutare a ridurre la superficie di attacco del cluster Redshift.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1	Modifica sempre le impostazioni predefinite del fornitore e rimuovi o disabilita gli account predefiniti non necessari prima di installare un sistema in rete. Ciò si applica a TUTTE le password predefinite, incluse, a titolo esemplificativo ma non esaustivo, quelle utilizzate dai sistemi operativi, dal software che fornisce servizi di sicurezza, dagli account di applicazione e di sistema, dai terminali point-of-sale (POS), dalle applicazioni di pagamento, dalle stringhe della community SNMP (Simple Network Management Protocol), ecc.).	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.1	Modifica sempre le impostazioni predefinite del fornitore e rimuovi o disabilita gli account predefiniti non necessari prima di installare un sistema in rete. Ciò vale per TUTTE le password predefinite, incluse, a titolo esemplificativo ma non esaustivo, quelle utilizzate dai sistemi operativi, dal software che fornisce servizi di sicurezza, gli account di applicazioni e di sistema, i terminali point-of-sale (POS), le applicazioni di pagamento, le stringhe di community SNMP (Simple Network Management Protocol), ecc.).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportare configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, ma non sono limitate a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	cloud-trail-log-file-validation-enabled	Utilizza AWS CloudTrail la convalida dei file di registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di protezione dei sistemi accettati dal settore possono includere , a titolo esemplifi cativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technolog y (NIST).	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	cmk-backing-key-rotation-enabled	Abilita la rotazione dei tasti per assicurarti che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, ma non sono limitate a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	ec2-instance-multiple-eni-check	Questa regola verifica se le istanze Amazon Elastic Compute Cloud (Amazon EC2) hanno più ENI. La presenza di più ENI può causare istanze dual-homed, ovvero istanze con più sottoreti. Ciò può aumentare la complessità della sicurezza della rete e introdurre percorsi e accessi di rete indesiderati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: «Center for Internet Security (CIS)» International Organization for Standardization (ISO) « SysAdmin Audit Network Security (SANS) Institute» National Institute of Standards Technology (NIST).	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, ma non sono limitate a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	ec2-security-group-attached-to-eni-periodic	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, ma non sono limitate a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, ma non sono limitate a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, ma non sono limitate a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, ma non sono limitate a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, ma non sono limitate a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: «Center for Internet Security (CIS)» International Organization for Standardization (ISO) « SysAdmin Audit Network Security (SANS) Institute» National Institute of Standards Technology (NIST).	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, ma non sono limitate a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, ma non sono limitate a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, ma non sono limitate a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2	Sviluppa standard di configurazione per tutti i componenti del sistema. Assicurarsi che questi standard risolvono tutte le vulnerabilità di sicurezza note e siano coerenti con gli standard di sicurezza del sistema accettati dal settore. Le fonti degli standard di rafforzamento dei sistemi accettati dal settore possono includere, a titolo esemplificativo ma non esaustivo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	restricted-ssh	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'acce sso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.2	Abilita solo i servizi, i protocolli, i daemon e altri elementi necessari per il funzionamento del sistema.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.2.3	Implementa funzionalità di sicurezza aggiuntive per tutti i servizi, i protocolli o i daemon richiesti considerati non sicuri.	alb-desync-mode-check	Per contribuire a proteggere le applicazioni dalle vulnerabilità della desincronizzazione HTTP, assicurati che la modalità di mitigazione della desincronizzazione HTTP sia abilitata sui sistemi di bilanciamento del carico delle applicazioni. I problemi di desincronizzazione HTTP possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della cache e della coda delle richieste. Le modalità di mitigazione della desincronizzazione sono Monitoraggio, Difensiva e Più rigorosa. Difensiva è la modalità predefinita.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.3	Crittografa tutti gli accessi amministr ativi non connessi alla console utilizzan do una crittografia avanzata.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
2.3	Crittografa tutti gli accessi amministr ativi non connessi alla console utilizzan do una crittografia avanzata.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.3	Crittografa tutti gli accessi amministr ativi non connessi alla console utilizzan do una crittografia avanzata.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
2.3	Crittografa tutti gli accessi amministr ativi non connessi alla console utilizzan do una crittografia avanzata.	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
2.3	Crittografa tutti gli accessi amministr ativi non connessi alla console utilizzan do una crittografia avanzata.	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittogra fia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per protegger e tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.4	Gestisci un inventario dei componenti di sistema che rientrano nell'ambito di PCI DSS.	ec2-security-group-attached-to-eni-periodic	Questa regola garantisce che i gruppi di sicurezza siano collegati a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o a un ENI. Questa regola aiuta a monitorare i gruppi di sicurezza inutilizzati nell'inventario e nella gestione dell'ambiente.
2.4	Gestisci un inventario dei componenti di sistema che rientrano nell'ambito di PCI DSS.	eip-attached	Questa regola garantisce che gli IP elastici allocati a un Amazon Virtual Private Cloud (Amazon VPC) siano collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) o a interfacce di rete elastiche in uso. Questa regola aiuta a monitorare gli EIP non utilizzati nel tuo ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.4	Gestisci un inventario dei componenti di sistema che rientrano nell'ambito di PCI DSS.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
2.4	Gestisci un inventario dei componenti di sistema che rientrano nell'ambito di PCI DSS.	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1	Mantieni al minimo l'archiviazione dei dati dei titolari di carta implementando policy, procedure e processi di conservazione e smaltimento dei dati che includano almeno quanto segue per l'archiviazione di tutti i dati dei titolari di carta (CHD): • Limitazione della quantità e del tempo di archiviazione dei dati a quanto indicato nei requisiti legali, normativi e/o aziendali • Requisiti di conservazione specifici per i dati dei titolari di carta • Processi per l'eliminazione sicura dei dati quando non sono più necessari • Un processo trimestrale per identificare ed eliminare in modo sicuro i dati dei titolari di carta archiviati che superano il limite di conservazione stabilito.	s3-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1	Mantieni al minimo l'archiviazione dei dati dei titolari di carta implementando policy, procedure e processi di conservazione e smaltimento dei dati che includano almeno quanto segue per l'archiviazione di tutti i dati dei titolari di carta (CHD): • Limitazione della quantità e del tempo di archiviazione dei dati a quanto indicato nei requisiti legali, normativi e/o aziendali • Requisiti di conservazione specifici per i dati dei titolari di carta • Processi per l'eliminazione sicura dei dati quando non sono più necessari • Un processo trimestrale per identificare ed eliminare in modo sicuro i dati dei titolari di carta archiviati che superano il limite di conservazione stabilito.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1	Mantieni al minimo l'archiviazione dei dati dei titolari di carta implementando policy, procedure e processi di conservazione e smaltimento dei dati che includano almeno quanto segue per l'archiviazione di tutti i dati dei titolari di carta (CHD): • Limitazione della quantità e del tempo di archiviazione dei dati a quanto indicato nei requisiti legali, normativi e/o aziendali • Requisiti di conservazione specifici per i dati dei titolari di carta • Processi per l'eliminazione sicura dei dati quando non sono più necessari • Un processo trimestrale per identificare ed eliminare in modo sicuro i dati dei titolari di carta archiviati che superano il limite di conservazione stabilito.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1	Mantieni al minimo l'archiviazione dei dati dei titolari di carta implementando policy, procedure e processi di conservazione e smaltimento dei dati che includano almeno quanto segue per l'archiviazione di tutti i dati dei titolari di carta (CHD): • Limitazione della quantità e del tempo di archiviazione dei dati a quanto indicato nei requisiti legali, normativi e/o aziendali • Requisiti di conservazione specifici per i dati dei titolari di carta • Processi per l'eliminazione sicura dei dati quando non sono più necessari • Un processo trimestrale per identificare ed eliminare in modo sicuro i dati dei titolari di carta archiviati che superano il limite di conservazione stabilito.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.4	Rendi il PAN illeggibile ovunque sia archiviato (inclusi supporti digitali portatili, supporti di backup e log) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncamento (l'hash non può essere utilizzato per sostituire il segmento di PAN troncato) • Token e pad indice (i pad devono essere archiviati in modo sicuro) • Crittografia avanzata con i processi e le procedure di gestione delle chiavi associati. Nota: per un utente malintenzionato che ha accesso sia alla versione troncata di un PAN sia a quella con hash, ricostruire i dati PAN originali è un'operazione	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	relativamente banale. Laddove nell'ambi ente di un'entità siano presenti versioni con hash e troncate dello stesso PAN, devono essere predisposti controlli aggiuntivi per garantire che le versioni con hash e troncate non possano essere correlate per ricostruire il PAN originale.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.2	Limita l'accesso alle chiavi crittografiche al minor numero di custodi necessario.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.2	Limita l'accesso alle chiavi crittografiche al minor numero di custodi necessario.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.3	Archivia sempre le chiavi segrete e private utilizzat e per crittografare/ decrittografare i dati dei titolari di carta in una (o più) delle seguenti forme: • Crittografate con una chiave di crittogra fia a chiave che sia almeno altrettanto potente della chiave di crittografia dei dati e archiviata separatamente dalla chiave di crittogra fia dei dati • All'inter no di un dispositivo crittografico sicuro (ad esempio un modulo di sicurezza hardware (host) (HSM) o un point-of-interaction dispositivo approvato da PTS) • Come in almeno due componenti chiave completi o condivisi oni di chiavi, secondo un metodo accettato dal settore Nota: non è necessario che le	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	chiavi pubbliche siano archiviate in uno dei questi moduli.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.3	Archivia sempre le chiavi segrete e private utilizzat e per crittografare/ decrittografare i dati dei titolari di carta in una (o più) delle seguenti forme: • Crittografate con una chiave di crittogra fia a chiave che sia almeno altrettanto potente della chiave di crittografia dei dati e archiviata separatamente dalla chiave di crittogra fia dei dati • All'inter no di un dispositivo crittografico sicuro (ad esempio un modulo di sicurezza hardware (host) (HSM) o un point-of-interaction dispositivo approvato da PTS) • Come in almeno due componenti chiave completi o condivisi oni di chiavi, secondo un metodo accettato dal settore Nota: non è necessario che le	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker endpoint. Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	chiavi pubbliche siano archiviate in uno dei questi moduli.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5.3	Archivia sempre le chiavi segrete e private utilizzat e per crittografare/ decrittografare i dati dei titolari di carta in una (o più) delle seguenti forme: • Crittografate con una chiave di crittogra fia a chiave che sia almeno altrettanto potente della chiave di crittografia dei dati e archiviata separatamente dalla chiave di crittogra fia dei dati • All'inter no di un dispositivo crittografico sicuro (ad esempio un modulo di sicurezza hardware (host) (HSM) o un point-of-interaction dispositivo approvato da PTS) • Come in almeno due componenti chiave completi o condivisi oni di chiavi, secondo un metodo accettato dal settore Nota: non è necessario che le	sagemaker-notebook -instance-kms-key-configured	Per proteggere i dati archiviati, assicurat i che la crittogra fia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	chiavi pubbliche siano archiviate in uno dei questi moduli.		
3.6.4	Modifica le chiavi crittografiche per le chiavi che hanno raggiunto la fine del loro periodo crittografico (ad esempio, dopo che è trascorso un determinato periodo di tempo e/o dopo che una determinata chiave ha prodotto una certa quantità di testo cifrato), come definito dal fornitore dell'applicazione associata o dal proprietario della chiave e in base alle best practice e alle linee guida del settore (ad esempio, NIST Special Publication 800-57).	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per garantire che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.5	Ritira o sostituisci (ad esempio, archivia, distruggi e/o revoca) le chiavi se ritenuto necessario o nei casi in cui l'integrità della chiave è stata indebolita (ad esempio, quando un dipendente che conosce un componente chiave in chiaro lascia l'azienda) o si sospetta che le chiavi siano compromesse. Nota: se è necessario conservare le chiavi crittografiche ritirate o sostituite, tali chiavi devono essere archiviate in modo sicuro (ad esempio, utilizzando una chiave di crittografia delle chiavi). Le chiavi crittografiche archiviate devono essere utilizzate solo per scopi di decrittografia/verifica.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.6.7	Previeni la sostituzione non autorizzata delle chiavi crittografiche.	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Utilizza una crittografia e protocolli di sicurezza avanzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche aperte, ad esempio: • Sono accettate solo chiavi e certificati affidabili. • Il protocollo in uso supporta solo versioni o configurazioni sicure. • Il livello di crittografia è appropriato per la metodologia di crittografia in uso. Esempi di reti pubbliche aperte includono, a titolo esemplificativo ma non esaustivo: • Internet • Tecnologie wireless, tra cui 802.11 e Bluetooth • Tecnologie cellulari, ad esempio Global System for Mobile communications (GSM), Code division multiple access	acm-certificate-expiration-check	Garantisci la protezione dell'integrità della rete assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(CDMA) • General Packet Radio Service (GPRS) • Comunicazioni via satellite.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Utilizza una crittografia e protocolli di sicurezza avanzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche aperte, ad esempio: • Sono accettate solo chiavi e certificati affidabili. • Il protocollo in uso supporta solo versioni o configurazioni sicure. • Il livello di crittografia è appropriato per la metodologia di crittografia in uso. Esempi di reti pubbliche aperte includono, a titolo esemplificativo ma non esaustivo: • Internet • Tecnologie wireless, tra cui 802.11 e Bluetooth • Tecnologie cellulari, ad esempio Global System for Mobile communications (GSM), Code division multiple access	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(CDMA) • General Packet Radio Service (GPRS) • Comunicazioni via satellite.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Utilizza una crittografia e protocolli di sicurezza avanzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche aperte, ad esempio: • Sono accettate solo chiavi e certificati affidabili. • Il protocollo in uso supporta solo versioni o configurazioni sicure. • Il livello di crittografia è appropriato per la metodologia di crittografia in uso. Esempi di reti pubbliche aperte includono, a titolo esemplificativo ma non esaustivo: • Internet • Tecnologie wireless, tra cui 802.11 e Bluetooth • Tecnologie cellulari, ad esempio Global System for Mobile communications (GSM), Code division multiple access	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(CDMA) • General Packet Radio Service (GPRS) • Comunicazioni via satellite.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Utilizza una crittografia e protocolli di sicurezza avanzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche aperte, ad esempio: • Sono accettate solo chiavi e certificati affidabili. • Il protocollo in uso supporta solo versioni o configurazioni sicure. • Il livello di crittografia è appropriato per la metodologia di crittografia in uso. Esempi di reti pubbliche aperte includono, a titolo esemplificativo ma non esaustivo: • Internet • Tecnologie wireless, tra cui 802.11 e Bluetooth • Tecnologie cellulari, ad esempio Global System for Mobile communications (GSM), Code division multiple access	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(CDMA) • General Packet Radio Service (GPRS) • Comunicazioni via satellite.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Utilizza una crittografia e protocolli di sicurezza avanzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche aperte, ad esempio: • Sono accettate solo chiavi e certificati affidabili. • Il protocollo in uso supporta solo versioni o configurazioni sicure. • Il livello di crittografia è appropriato per la metodologia di crittografia in uso. Esempi di reti pubbliche aperte includono, a titolo esemplificativo ma non esaustivo: • Internet • Tecnologie wireless, tra cui 802.11 e Bluetooth • Tecnologie cellulari, ad esempio Global System for Mobile communications (GSM), Code division multiple access	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(CDMA) • General Packet Radio Service (GPRS) • Comunicazioni via satellite.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Utilizza una crittografia e protocolli di sicurezza avanzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche aperte, ad esempio: • Sono accettate solo chiavi e certificati affidabili. • Il protocollo in uso supporta solo versioni o configurazioni sicure. • Il livello di crittografia è appropriato per la metodologia di crittografia in uso. Esempi di reti pubbliche aperte includono, a titolo esemplificativo ma non esaustivo: • Internet • Tecnologie wireless, tra cui 802.11 e Bluetooth • Tecnologie cellulari, ad esempio Global System for Mobile communications (GSM), Code division multiple access	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(CDMA) • General Packet Radio Service (GPRS) • Comunicazioni via satellite.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Utilizza una crittografia e protocolli di sicurezza avanzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche aperte, ad esempio: • Sono accettate solo chiavi e certificati affidabili. • Il protocollo in uso supporta solo versioni o configurazioni sicure. • Il livello di crittografia è appropriato per la metodologia di crittografia in uso. Esempi di reti pubbliche aperte includono, a titolo esemplificativo ma non esaustivo: • Internet • Tecnologie wireless, tra cui 802.11 e Bluetooth • Tecnologie cellulari, ad esempio Global System for Mobile communications (GSM), Code division multiple access	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(CDMA) • General Packet Radio Service (GPRS) • Comunicazioni via satellite.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Utilizza una crittografia e protocolli di sicurezza avanzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche aperte, ad esempio: • Sono accettate solo chiavi e certificati affidabili. • Il protocollo in uso supporta solo versioni o configurazioni sicure. • Il livello di crittografia è appropriato per la metodologia di crittografia in uso. Esempi di reti pubbliche aperte includono, a titolo esemplificativo ma non esaustivo: • Internet • Tecnologie wireless, tra cui 802.11 e Bluetooth • Tecnologie cellulari, ad esempio Global System for Mobile communications (GSM), Code division multiple access	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(CDMA) • General Packet Radio Service (GPRS) • Comunicazioni via satellite.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Utilizza una crittografia e protocolli di sicurezza avanzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche aperte, ad esempio: • Sono accettate solo chiavi e certificati affidabili. • Il protocollo in uso supporta solo versioni o configurazioni sicure. • Il livello di crittografia è appropriato per la metodologia di crittografia in uso. Esempi di reti pubbliche aperte includono, a titolo esemplificativo ma non esaustivo: • Internet • Tecnologie wireless, tra cui 802.11 e Bluetooth • Tecnologie cellulari, ad esempio Global System for Mobile communications (GSM), Code division multiple access	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(CDMA) • General Packet Radio Service (GPRS) • Comunicazioni via satellite.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.1	Utilizza una crittografia e protocolli di sicurezza avanzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche aperte, ad esempio: • Sono accettate solo chiavi e certificati affidabili. • Il protocollo in uso supporta solo versioni o configurazioni sicure. • Il livello di crittografia è appropriato per la metodologia di crittografia in uso. Esempi di reti pubbliche aperte includono, a titolo esemplificativo ma non esaustivo: • Internet • Tecnologie wireless, tra cui 802.11 e Bluetooth • Tecnologie cellulari, ad esempio Global System for Mobile communications (GSM), Code division multiple access	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(CDMA) • General Packet Radio Service (GPRS) • Comunicazioni via satellite.		
6.2	Assicurati che tutti i componenti di sistema e il software siano protetti da vulnerabilità note installando le patch di sicurezza applicabili fornite dal fornitore. Installare le patch di sicurezza critiche entro un mese dal rilascio. Nota: le patch di sicurezza critiche devono essere identificate in base al processo di classificazione del rischio definito nel Requisito 6.1.	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.2	Assicurati che tutti i componenti di sistema e il software siano protetti da vulnerabilità note installando le patch di sicurezza applicabili fornite dal fornitore. Installare le patch di sicurezza critiche entro un mese dal rilascio. Nota: le patch di sicurezza critiche devono essere identificate in base al processo di classificazione del rischio definito nel Requisito 6.1.	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.2	Assicurati che tutti i componenti di sistema e il software siano protetti da vulnerabilità note installando le patch di sicurezza applicabili fornite dal fornitore. Installare le patch di sicurezza critiche entro un mese dal rilascio. Nota: le patch di sicurezza critiche devono essere identificate in base al processo di classificazione del rischio definito nel Requisito 6.1.	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.2	Assicurati che tutti i componenti di sistema e il software siano protetti da vulnerabilità note installando le patch di sicurezza applicabili fornite dal fornitore. Installare le patch di sicurezza critiche entro un mese dal rilascio. Nota: le patch di sicurezza critiche devono essere identificate in base al processo di classificazione del rischio definito nel Requisito 6.1.	ecs-fargate-latest-platform-version	Gli aggiornamenti e le patch di sicurezza vengono distribuiti automaticamente per le attività di Fargate AWS . Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma AWS Fargate, AWS corregge la versione della piattaforma. Per aiutarti nella gestione delle patch delle attività di Amazon Elastic Container Service (ECS) che eseguono AWS Fargate, aggiorna le attività autonome dei servizi per utilizzare la versione più recente della piattaforma.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.2	Assicurati che tutti i componenti di sistema e il software siano protetti da vulnerabilità note installando le patch di sicurezza applicabili fornite dal fornitore. Installare le patch di sicurezza critiche entro un mese dal rilascio. Nota: le patch di sicurezza critiche devono essere identificate in base al processo di classificazione del rischio definito nel Requisito 6.1.	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.2	Assicurati che tutti i componenti di sistema e il software siano protetti da vulnerabilità note installando le patch di sicurezza applicabili fornite dal fornitore. Installare le patch di sicurezza critiche entro un mese dal rilascio. Nota: le patch di sicurezza critiche devono essere identificate in base al processo di classificazione del rischio definito nel Requisito 6.1.	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3.2	Rivedi il codice personalizzato prima di rilasciarlo in produzione o ai clienti per identificare eventuali vulnerabilità di codifica (utilizzando processi manuali o automatizzati) e includere almeno quanto segue: • Le modifiche al codice vengono esaminate da persone diverse dall'autore del codice originale e da persone esperte sulle tecniche di revisione del codice e sulle pratiche di codifica sicure. • Le revisioni del codice garantiscono che il codice sia sviluppato secondo linee guida di codifica sicura • Le correzioni appropriate vengono apportate prima del rilascio. • I risultati della revisione del codice vengono esaminati e approvati dalla direzione prima del rilascio.	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilitazione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	(continua nella pagina successiva)		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.6	Per le applicazioni Web rivolte al pubblico, affronta costantemente nuove minacce e vulnerabilità e assicurati che tali applicazioni siano protette dagli attacchi noti con uno dei seguenti metodi: • Revisione delle applicazioni Web rivolte al pubblico tramite strumenti o metodi manuali o automatizzati di valutazione della sicurezza e delle vulnerabilità delle applicazioni, almeno una volta all'anno e dopo eventuali modifiche. Nota: questa valutazione non coincide con le scansioni delle vulnerabilità eseguite per il Requisito 11.2. • Installazione di una soluzione tecnica automatizzata che rileva e previene gli attacchi basati sul	alb-desync-mode-check	Per contribuire a proteggere le applicazioni dalle vulnerabilità della desincronizzazione HTTP, assicurati che la modalità di mitigazione della desincronizzazione HTTP sia abilitata sui sistemi di bilanciamento del carico delle applicazioni. I problemi di desincronizzazione HTTP possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della cache e della coda delle richieste. Le modalità di mitigazione della desincronizzazione sono Monitoraggio, Difensiva e Più rigorosa. Difensiva è la modalità predefinita.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Web (ad esempio, un firewall per applicazioni Web) davanti alle applicazioni Web rivolte al pubblico, per controllare continuamente tutto il traffico.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.6	Per le applicazioni Web rivolte al pubblico, affronta costantemente nuove minacce e vulnerabilità e assicurati che tali applicazioni siano protette dagli attacchi noti con uno dei seguenti metodi: • Revisione delle applicazioni Web rivolte al pubblico tramite strumenti o metodi manuali o automatizzati di valutazione della sicurezza e delle vulnerabilità delle applicazioni, almeno una volta all'anno e dopo eventuali modifiche. Nota: questa valutazione non coincide con le scansioni delle vulnerabilità eseguite per il Requisito 11.2. • Installazione di una soluzione tecnica automatizzata che rileva e previene gli attacchi basati sul	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Web (ad esempio, un firewall per applicazi oni Web) davanti alle applicazioni Web rivolte al pubblico, per controllare continuam ente tutto il traffico.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.6	Per le applicazioni Web rivolte al pubblico, affronta costantemente nuove minacce e vulnerabilità e assicurati che tali applicazioni siano protette dagli attacchi noti con uno dei seguenti metodi: • Revisione delle applicazioni Web rivolte al pubblico tramite strumenti o metodi manuali o automatizzati di valutazione della sicurezza e delle vulnerabilità delle applicazioni, almeno una volta all'anno e dopo eventuali modifiche. Nota: questa valutazione non coincide con le scansioni delle vulnerabilità eseguite per il Requisito 11.2. • Installazione di una soluzione tecnica automatizzata che rileva e previene gli attacchi basati sul	api-gw-associated-with-waf	AWS WAF consente di configurare un insieme di regole (chiamate elenco di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Web (ad esempio, un firewall per applicazi oni Web) davanti alle applicazioni Web rivolte al pubblico, per controllare continuam ente tutto il traffico.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.6	Per le applicazioni Web rivolte al pubblico, affronta costantemente nuove minacce e vulnerabilità e assicurati che tali applicazioni siano protette dagli attacchi noti con uno dei seguenti metodi: • Revisione delle applicazioni Web rivolte al pubblico tramite strumenti o metodi manuali o automatizzati di valutazione della sicurezza e delle vulnerabilità delle applicazioni, almeno una volta all'anno e dopo eventuali modifiche. Nota: questa valutazione non coincide con le scansioni delle vulnerabilità eseguite per il Requisito 11.2. • Installazione di una soluzione tecnica automatizzata che rileva e previene gli attacchi basati sul	waf-regional-rule-not-empty	Assicurati che il tuo AWS WAF abbia una regola che non sia vuota. Una regola senza condizioni può comportare un comportamento non intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Web (ad esempio, un firewall per applicazioni Web) davanti alle applicazioni Web rivolte al pubblico, per controllare continuamente tutto il traffico.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.6	Per le applicazioni Web rivolte al pubblico, affronta costantemente nuove minacce e vulnerabilità e assicurati che tali applicazioni siano protette dagli attacchi noti con uno dei seguenti metodi: • Revisione delle applicazioni Web rivolte al pubblico tramite strumenti o metodi manuali o automatizzati di valutazione della sicurezza e delle vulnerabilità delle applicazioni, almeno una volta all'anno e dopo eventuali modifiche. Nota: questa valutazione non coincide con le scansioni delle vulnerabilità eseguite per il Requisito 11.2. • Installazione di una soluzione tecnica automatizzata che rileva e previene gli attacchi basati sul	waf-regional-rulegroup-not-empty	Assicurati che il tuo AWS WAF abbia un gruppo di regole che non sia vuoto. Un gruppo di regole vuoto potrebbe causare un comportamento indesiderato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Web (ad esempio, un firewall per applicazioni Web) davanti alle applicazioni Web rivolte al pubblico, per controllare continuamente tutto il traffico.		

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.6	Per le applicazioni Web rivolte al pubblico, affronta costantemente nuove minacce e vulnerabilità e assicurati che tali applicazioni siano protette dagli attacchi noti con uno dei seguenti metodi: • Revisione delle applicazioni Web rivolte al pubblico tramite strumenti o metodi manuali o automatizzati di valutazione della sicurezza e delle vulnerabilità delle applicazioni, almeno una volta all'anno e dopo eventuali modifiche. Nota: questa valutazione non coincide con le scansioni delle vulnerabilità eseguite per il Requisito 11.2. • Installazione di una soluzione tecnica automatizzata che rileva e previene gli attacchi basati sul	waf-regional-webacl-not-empty	Un ACL Web collegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
	Web (ad esempio, un firewall per applicazioni Web) davanti alle applicazioni Web rivolte al pubblico, per controllare continuamente tutto il traffico.		
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanism i di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzar e le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	ecs-containers-non privileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	efs-access-point-enforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.1	Definisci le esigenze di accesso per ogni ruolo, tra cui: • Componenti di sistema e risorse di dati a cui ogni ruolo deve accedere per la propria funzione lavorativa • Livello di privilegio richiesto (ad esempio, utente, amministratore e così via) per accedere alle risorse.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearch

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.2	Limita l'accesso agli ID utente con privilegi ai privilegi minimi necessari per svolgere le mansioni lavorative.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.2	Limita l'accesso agli ID utente con privilegi ai privilegi minimi necessari per svolgere le mansioni lavorative.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.2	Limita l'accesso agli ID utente con privilegi ai privilegi minimi necessari per svolgere le mansioni lavorative.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
7.1.2	Limita l'accesso agli ID utente con privilegi ai privilegi minimi necessari per svolgere le mansioni lavorative.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.2	Limita l'accesso agli ID utente con privilegi ai privilegi minimi necessari per svolgere le mansioni lavorative.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.2	Limita l'accesso agli ID utente con privilegi ai privilegi minimi necessari per svolgere le mansioni lavorative.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
71.2	Limita l'accesso agli ID utente con privilegi ai privilegi minimi necessari per svolgere le mansioni lavorative.	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.1.2	Limita l'accesso agli ID utente con privilegi ai privilegi minimi necessari per svolgere le mansioni lavorative.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
7.1.2	Limita l'accesso agli ID utente con privilegi ai privilegi minimi necessari per svolgere le mansioni lavorative.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprendere quanto segue: copertura di tutti i componenti del sistema.	ecs-containers-non privileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizioni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprendere quanto segue: copertura di tutti i componenti del sistema.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprende re quanto segue: copertura di tutti i componenti del sistema.	efs-access-point-e nforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprendere quanto segue: copertura di tutti i componenti del sistema.	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprende re quanto segue: copertura di tutti i componenti del sistema.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprendere quanto segue: copertura di tutti i componenti del sistema.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatterns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprendere quanto segue: copertura di tutti i componenti del sistema.	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicurando che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprendere quanto segue: copertura di tutti i componenti del sistema.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms:ReEncrypt From). I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprendere quanto segue: copertura di tutti i componenti del sistema.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprendere quanto segue: copertura di tutti i componenti del sistema.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprende re quanto segue: copertura di tutti i componenti del sistema.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprende re quanto segue: copertura di tutti i componenti del sistema.	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprendere quanto segue: copertura di tutti i componenti del sistema.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprende re quanto segue: copertura di tutti i componenti del sistema.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.1	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. I sistemi di controllo degli accessi devono comprende re quanto segue: copertura di tutti i componenti del sistema.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearc h

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classific azione e alla funzione professionali.	ecs-containers-non privileged	Per facilitare l'implementazione del principio del privilegio minimo, non devono essere abilitati privilegi elevati per le definizio ni delle attività Amazon Elastic Container Service (Amazon ECS). Se il parametro è true, al container vengono assegnati privilegi elevati nell'istanza di container host (simile all'utente root).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classificazione e alla funzione professionali.	ecs-containers-readonly-access	L'abilitazione dell'accesso in sola lettura ai container Amazon Elastic Container Service (ECS) può aiutare a rispettare il principio del privilegio minimo. Questa opzione può ridurre i vettori di attacco poiché il file system dell'istanza di container non può essere modificato a meno che non disponga di autorizzazioni esplicite di lettura/scrittura.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classific azione e alla funzione professionali.	efs-access-point-e nforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classific azione e alla funzione professionali.	efs-access-point-e nforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'uten te sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazion i sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classific azione e alla funzione professionali.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classific azione e alla funzione professionali.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazio ne dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti. Questa regola consente di impostare il parametro . blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decry pt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classific azione e alla funzione professionali.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classific azione e alla funzione professionali.	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni. Questa regola consente di impostare il blockedActionsPatt erns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			riflettere le policy dell'organizzazione.
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classific azione e alla funzione professionali.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classificazione e alla funzione professionali.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo che le policy contengano «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classific azione e alla funzione professionali.	iam-policy-no-stat ements-with-full-a ccess	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classific azione e alla funzione professionali.	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classificazione e alla funzione professionali.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classific azione e alla funzione professionali.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.2	Stabilisci un sistema di controllo degli accessi per i componenti di sistema che limiti l'accesso in base alla necessità di sapere dell'utente e che sia impostato su "nega tutti", a meno che non sia espressamente consentito. Questi sistemi di controllo degli accessi devono includere quanto segue: assegnazione di privilegi agli utenti in base alla classific azione e alla funzione professionali.	opensearch-access-control-enabled	Assicurati che il controllo granulare degli accessi sia abilitato sui tuoi domini Amazon OpenSearch Service. Il controllo granulare degli accessi fornisce meccanismi di autorizzazione avanzati per ottenere l'accesso con i privilegi minimi ai domini di Amazon Service. OpenSearch Consente il controllo degli accessi al dominio in base ai ruoli, nonché la sicurezza a livello di indice, documento e campo, il supporto per dashboard di servizio multi-tenancy e l'autenticazione di base HTTP per OpenSearch Service e Kibana. OpenSearc h

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
7.2.3	Impostazione predefinita "deny-all".	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanism i di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzar e le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1.1	Assegna a tutti gli utenti un ID univoco prima di consentir e loro di accedere ai componenti del sistema o ai dati dei titolari di carta.	iam-root-access-key-check	L'accesso ai sistemi e alle risorse può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate . Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzional ità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1.4	Rimuovere/disabilitare gli account utente inattivi entro 90 giorni.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	codebuild-project-environment-privileged-check	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che il tuo ambiente di CodeBuild progetto Amazon non abbia la modalità privilegiata abilitata. Questa impostazione deve essere disabilitata per impedire l'accesso involontario alle API Docker e all'hardware sottostante del container.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	ecs-no-environment-secrets	Come best practice per la sicurezza, trasferisci le informazioni sensibili ai container come variabili di ambiente. Puoi inserire dati in modo sicuro nei tuoi contenitori Amazon Elastic Container Service (ECS) facendo riferimento ai valori memorizzati in AWS Systems Manager Parameter Store o Secrets Manager nella AWS definizione del contenitore di una definizione di attività Amazon ECS. Puoi quindi esporre le tue informazioni sensibili come variabili di ambiente o nella configurazione di log di un container.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a memoria inattiva per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.1	Utilizzando crittografia avanzata, eseguire il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
8.2.1	Utilizzando crittografia avanzata, eseguire il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.1	Utilizzando crittografia avanzata, esegui il rendering di tutte le credenziali di autenticazione illeggibili (ad esempio password/frasi) durante la trasmissione e l'archiviazione su tutti i componenti di sistema.	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.3	Le password/passphrase devono soddisfare i seguenti requisiti: • Richieder e una lunghezza minima di almeno sette caratteri. • Contenere sia caratteri numerici che alfabetici. In alternati va, le password/passphrase devono avere una complessi tà e una robustezza almeno equivalenti ai parametri specificati sopra.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'orga nizzazione. Soddisfan o o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltati vamente RequireUp percaseCharacters (impostazione PCI DSS: false), RequireLowercaseCh aracters (impostaz ione PCI DSS predefinita: true), RequireSymbols (impostazione PCI DSS predefinita: false), RequireNu mbers (impostazione PCI DSS predefini ta: true), MinimumPa sswordLength

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(impostazione PCI DSS predefinita: 7), PasswordReusePrevention (impostazione PCI DSS predefinita: 4) e MaxPasswordAge (impostazione PCI DSS predefinita: 90) per la politica delle password IAM. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.4	Modificare le password/passphrase degli utenti almeno ogni 90 giorni.	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.4	Modifica le password/passphrase degli utenti almeno ogni 90 giorni.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard Foundational Security Best Practices per la sicurezza delle password. AWS Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (impostazione PCI DSS: false), RequireLowercaseCharacters (impostazione PCI DSS predefinita: true), RequireSymbols (impostazione PCI DSS predefinita: false), RequireNumbers (impostazione PCI DSS predefinita: true), MinimumPasswordLength

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(impostazione PCI DSS predefinita: 7), PasswordReusePreve ntion (impostazione PCI DSS predefini ta: 4) e MaxPasswo rdAge (impostazione PCI DSS predefini ta: 90) per la politica delle password IAM. I valori effettivi devono riflettere le policy dell'organizzazione.
8.2.4	Modificare le password/passphras e degli utenti almeno ogni 90 giorni.	secretsmanager-rot ation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianifica zione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromis sione del segreto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.2.5	Non consentire a nessuno di inviare una nuova password/passphrase uguale a una delle ultime quattro password/passphrase utilizzate.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (impostazione PCI DSS: false), RequireLowercaseCharacters (impostazione PCI DSS predefinita: true), RequireSymbols (impostazione PCI DSS predefinita: false), RequireNumbers (impostazione PCI DSS predefinita: true), MinimumPasswordLength

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(impostazione PCI DSS predefinita: 7), PasswordReusePreve ntion (impostazione PCI DSS predefini ta: 4) e MaxPasswo rdAge (impostazione PCI DSS predefini ta: 90) per la politica delle password IAM. I valori effettivi devono riflettere le policy dell'organizzazione.
8.3.1	Incorpora l'autenti cazione a più fattori per tutti gli accessi non associati alla console nel CDE per il personale con accesso amministr ativo.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromis sione degli account richiedendo l'autenti cazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.3.1	Incorpora l'autenticazione a più fattori per tutti gli accessi non associati alla console nel CDE per il personale con accesso amministrativo.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.3.1	Incorpora l'autenticazione a più fattori per tutti gli accessi non associati alla console nel CDE per il personale con accesso amministrativo.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.3.1	Incorpora l'autenticazione a più fattori per tutti gli accessi non associati alla console nel CDE per il personale con accesso amministrativo.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.3.2	Incorpora l'autenticazione a più fattori per tutti gli accessi remoti alla rete (utente e amministratore e anche l'accesso di terze parti per il supporto o la manutenzione) provenienti dall'esterno della rete dell'entità.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.3.2	Incorpora l'autenticazione a più fattori per tutti gli accessi remoti alla rete (utente e amministratore e anche l'accesso di terze parti per il supporto o la manutenzione) provenienti dall'esterno della rete dell'entità.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongono di una password di console. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromissione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.3.2	Incorpora l'autenticazione a più fattori per tutti gli accessi remoti alla rete (utente e amministratore e anche l'accesso di terze parti per il supporto o la manutenzione) provenienti dall'esterno della rete dell'entità.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.3.2	Incorpora l'autenticazione a più fattori per tutti gli accessi remoti alla rete (utente e amministratore e anche l'accesso di terze parti per il supporto o la manutenzione) provenienti dall'esterno della rete dell'entità.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per nome utente e password. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.1	Implementa gli audit trail per collegare tutti gli accessi ai componenti di sistema a ogni singolo utente.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.1	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tutti i singoli utenti accedono ai dati del titolare della carta.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.1	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tutti i singoli utenti accedono ai dati del titolare della carta.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.1	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tutti i singoli utenti accedono ai dati del titolare della carta.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.1	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tutti i singoli utenti accedono ai dati del titolare della carta.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
10.2.1	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tutti i singoli utenti accedono ai dati del titolare della carta.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.1	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tutti i singoli utenti accedono ai dati del titolare della carta.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.1	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tutti i singoli utenti accedono ai dati del titolare della carta.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.1	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tutti i singoli utenti accedono ai dati del titolare della carta.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.1	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tutti i singoli utenti accedono ai dati del titolare della carta.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.1	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostrui re gli eventi seguenti: tutti i singoli utenti accedono ai dati del titolare della carta.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.1	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tutti i singoli utenti accedono ai dati del titolare della carta.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.2	Implementa audit trail automatizzati per tutti i component i di sistema per ricostruire gli eventi seguenti: tutte le azioni intraprese da qualsiasi persona con privilegi root o amministrativi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indiriz zo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrai l consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrai l Di conseguenza, riceverai file di log contenenti l'attivit à delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.2	Implementa audit trail automatizzati per tutti i component i di sistema per ricostruire gli eventi seguenti: tutte le azioni intraprese da qualsiasi persona con privilegi root o amministrativi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.2	Implementa audit trail automatizzati per tutti i component i di sistema per ricostruire gli eventi seguenti: tutte le azioni intraprese da qualsiasi persona con privilegi root o amministrativi.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatc h Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazi oni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.2	Implementa audit trail automatizzati per tutti i component i di sistema per ricostruire gli eventi seguenti: tutte le azioni intraprese da qualsiasi persona con privilegi root o amministrativi.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearc h di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservaz ione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibi lità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.2	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tutte le azioni intraprese da qualsiasi persona con privilegi root o amministrativi.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.2	Implementa audit trail automatizzati per tutti i component i di sistema per ricostruire gli eventi seguenti: tutte le azioni intraprese da qualsiasi persona con privilegi root o amministrativi.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearc h di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearc h I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosti care problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.2	Implementa audit trail automatizzati per tutti i component i di sistema per ricostruire gli eventi seguenti: tutte le azioni intraprese da qualsiasi persona con privilegi root o amministrativi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.2	Implementa audit trail automatizzati per tutti i component i di sistema per ricostruire gli eventi seguenti: tutte le azioni intraprese da qualsiasi persona con privilegi root o amministrativi.	redshift-cluster-c onfiguration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificar e che le configura zioni richieste siano implementate sui cluster Amazon Redshift. La registraz ione di log di audit deve essere abilitata per fornire informazi oni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDb Encrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.3	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: accesso a tutti gli audit trail.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.3	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: accesso a tutti gli audit trail.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
10.2.3	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: accesso a tutti gli audit trail.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.3	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: accesso a tutti gli audit trail.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.3	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: accesso a tutti gli audit trail.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.3	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: accesso a tutti gli audit trail.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.3	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: accesso a tutti gli audit trail.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.3	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostrui re gli eventi seguenti: accesso a tutti gli audit trail.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2,3	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: accesso a tutti gli audit trail.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.3	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: accesso a tutti gli audit trail.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.4	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tentativi di accesso logico non validi.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.4	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tentativi di accesso logico non validi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.4	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tentativi di accesso logico non validi.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.4	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tentativi di accesso logico non validi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
10.2.4	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tentativi di accesso logico non validi.	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.4	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tentativi di accesso logico non validi.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.4	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tentativi di accesso logico non validi.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.4	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tentativi di accesso logico non validi.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.4	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tentativi di accesso logico non validi.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.4	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostrui re gli eventi seguenti: tentativi di accesso logico non validi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.4	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: tentativi di accesso logico non validi.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.5	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: utilizzo e modifiche di meccanismi di identificazione e autenticazione, inclusi, a titolo esemplificativo, la creazione di nuovi account e l'aumento dei privilegi, e tutte le modifiche, aggiunte o eliminazioni agli account con privilegi root o amministrativi.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.5	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: utilizzo e modifiche di meccanismi di identificazione e autenticazione, inclusi, a titolo esemplificativo, la creazione di nuovi account e l'aumento dei privilegi, e tutte le modifiche, aggiunte o eliminazioni agli account con privilegi root o amministrativi.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.5	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: utilizzo e modifiche di meccanismi di identificazione e autenticazione, inclusi, a titolo esemplificativo, la creazione di nuovi account e l'aumento dei privilegi, e tutte le modifiche, aggiunte o eliminazioni agli account con privilegi root o amministrativi.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.5	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: utilizzo e modifiche di meccanismi di identificazione e autenticazione, inclusi, a titolo esemplificativo, la creazione di nuovi account e l'aumento dei privilegi, e tutte le modifiche, aggiunte o eliminazioni agli account con privilegi root o amministrativi.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.5	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: utilizzo e modifiche di meccanismi di identificazione e autenticazione, inclusi, a titolo esemplificativo, la creazione di nuovi account e l'aumento dei privilegi, e tutte le modifiche, aggiunte o eliminazioni agli account con privilegi root o amministrativi.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.5	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: utilizzo e modifiche di meccanismi di identificazione e autenticazione, inclusi, a titolo esemplificativo, la creazione di nuovi account e l'aumento dei privilegi, e tutte le modifiche, aggiunte o eliminazioni agli account con privilegi root o amministrativi.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.5	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostrui re gli eventi seguenti: utilizzo e modifiche di meccanismi di identificazione e autenticazione, inclusi, a titolo esemplificativo, la creazione di nuovi account e l'aumento dei privilegi, e tutte le modifiche, aggiunte o eliminazioni agli account con privilegi root o amministrativi.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
102,5	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: utilizzo e modifiche di meccanismi di identificazione e autenticazione, inclusi, a titolo esemplificativo, la creazione di nuovi account e l'aumento dei privilegi, e tutte le modifiche, aggiunte o eliminazioni agli account con privilegi root o amministrativi.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.6	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: inizializzazione, arresto o sospensione dei log di audit.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.6	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: inizializzazione, arresto o sospensione dei log di audit.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.6	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: inizializzazione, arresto o sospensione dei log di audit.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
10,27	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: creazione ed eliminazione di oggetti a livello di sistema.	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,27	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: creazione ed eliminazione di oggetti a livello di sistema.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.7	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: creazione ed eliminazione di oggetti a livello di sistema.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.7	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: creazione ed eliminazione di oggetti a livello di sistema.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.7	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: creazione ed eliminazione di oggetti a livello di sistema.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.7	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostruire gli eventi seguenti: creazione ed eliminazione di oggetti a livello di sistema.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.2.7	Implementa audit trail automatizzati per tutti i componenti di sistema per ricostrui re gli eventi seguenti: creazione ed eliminazi one di oggetti a livello di sistema.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
103,1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	api-gw-execution-l ogging-enabled	La registrazione di log di Gateway API mostra viste dettaglia te degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identific are gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	cloudtrail-s3-data events-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.3.1	Registra almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento: identificazione utente.	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.5	Proteggi gli audit trail in modo che non possano essere modificati.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi percorsi. AWS CloudTrail
10.5	Proteggi gli audit trail in modo che non possano essere modificati.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.5	Proteggi gli audit trail in modo che non possano essere modificati.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
10.5.2	Proteggi i file di audit trail da modifiche non autorizzate.	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurat i che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.5.2	Proteggi i file di audit trail da modifiche non autorizzate.	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittogra fia per proteggere tali dati.
10,5,2	Proteggi i file di audit trail da modifiche non autorizzate.	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,5,3	Esegui il backup tempestivo dei file di audit trail in un server di log centralizzato o un supporto che è difficile da modificare.	s3-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,5,3	Esegui il backup tempestivo dei file di audit trail in un server di log centralizzato o un supporto che è difficile da modificare.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
10.5.3	Esegui il backup tempestivo dei file di audit trail in un server di log centralizzato o un supporto che è difficile da modificare.	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
10.5.3	Esegui il backup tempestivo dei file di audit trail in un server di log centralizzato o un supporto che è difficile da modificare.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenime nto di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10,5,5	Utilizza il software di monitoraggio dell'integrità dei file o di rilevamento delle modifiche nei log per garantire che i dati di log esistenti non possano essere modificati senza generare avvisi (anche se l'aggiunta di nuovi dati non deve causare avvisi).	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.5.5	Utilizza il software di monitoraggio dell'integrità dei file o di rilevamento delle modifiche nei log per garantire che i dati di log esistenti non possano essere modificati senza generare avvisi (anche se l'aggiunta di nuovi dati non deve causare avvisi).	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.7	Conserva la cronologia degli audit trail per almeno un anno, con un minimo di tre mesi di disponibilità immediata per l'analisi (ad esempio online, archiviata o ripristinabile dal backup).	s3-lifecycle-policy-check	Assicurati che le policy del ciclo di vita Amazon S3 siano configurate per definire le operazioni che deve eseguire Amazon S3 durante il ciclo di vita di un oggetto, ad esempio la transizione di oggetti in un'altra classe di storage, la relativa archiviazione o l'eliminazione dopo un periodo di tempo specificato.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
10.7	Conserva la cronologia degli audit trail per almeno un anno, con un minimo di tre mesi di disponibilità immediata per l'analisi (ad esempio online, archiviata o ripristinabile dal backup).	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
11.2.3	Esegui scansioni interne ed esterne e, se necessario, ripeti le scansioni dopo ogni modifica significativa. Le scansioni devono essere eseguite da personale qualificato.	ecr-private-image-scanning-enabled	La scansione delle immagini di Amazon Elastic Container Repository (ECR) aiuta a identificare le vulnerabilità software nelle immagini dei container. L'abilita zione della scansione delle immagini sui repository ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Utilizza tecniche di rilevamento e/o prevenzione delle intrusioni per rilevare e/o prevenire le intrusioni nella rete. Monitora tutto il traffico lungo il perimetro e nei punti critici dell'ambiente dati del titolare della carta e avvisa il personale in caso di sospette compromis sioni. Mantieni aggiornati tutti i motori, le linee di base e le firme per il rilevamento e la prevenzione delle intrusioni.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.4	Utilizza tecniche di rilevamento e/o prevenzione delle intrusioni per rilevare e/o prevenire le intrusioni nella rete. Monitora tutto il traffico lungo il perimetro e nei punti critici dell'ambiente dati del titolare della carta e avvisa il personale in caso di sospette compromis sioni. Mantieni aggiornati tutti i motori, le linee di base e le firme per il rilevamento e la prevenzione delle intrusioni.	netfw-policy-rule-group-associated	Una policy AWS Network Firewall definisce il modo in cui il firewall monitora e gestisce il traffico in un Amazon VPC. Puoi configurare gruppi di regole stateless e stateful per filtrare pacchetti e flussi di traffico, nonché definire la gestione del traffico predefinita.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.5	Implementa un meccanismo di rilevamento delle modifiche (ad esempio strumenti di monitoraggio dell'integrità dei file) per avvisare il personale in caso di modifiche non autorizzate (incluse modifiche, aggiunte ed eliminazioni) di file di sistema, file di configurazione o file di contenuto critici e configura il software in modo da eseguire confronti tra file critici almeno una volta alla settimana.	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei log. CloudTrail La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
11.5	Implementa un meccanismo di rilevamento delle modifiche (ad esempio strumenti di monitoraggio dell'integrità dei file) per avvisare il personale in caso di modifiche non autorizzate (incluse modifiche, aggiunte ed eliminazioni) di file di sistema, file di configurazione o file di contenuto critici e configura il software in modo da eseguire confronti tra file critici almeno una volta alla settimana.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

Modello

Il modello è disponibile su GitHub: Operational Best Practices for PCI DSS 3.2.1.

Best practice operative per risorse accessibili pubblicamente

Questo pacchetto di conformità aiuta a identificare le risorse che possono essere accessibili pubblicamente.

Per un elenco di tutte le regole gestite supportate da AWS Config, vedere Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Migliori pratiche operative per risorse accessibili al pubblico.

Best practice operative per RBI Cyber Security Framework per UCB

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il Cyber Security Framework for Urban Cooperative Banks (UCB) della Reserve Bank of India (RBI) e le regole Config gestite AWS . Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli RBI Cyber Security Framework for UCbs. Un controllo RBI Cyber Security Framework per UCB può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.1)	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore

ID controllo	AWS Regola di Config	Linea guida
		e versione e altri dettagli sull'ambiente.
Annex_I(1.1)	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportar e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.
Annex_I(1.1)	ecr-private-tag-immutability-enabled	Abilita l'immutabilità dei tag di Elastic Container Repositor y (ECR) per evitare che i tag di immagine sulle immagini ECR vengano sovrascritti. In precedenza, i tag potevano essere sovrascritti, richieden do metodologie manuali per identificare in modo univoco un'immagine.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	acm-certificate-expiration-check	Garantisci la protezion e dell'integrità della rete assicurando che i certifica ti X509 vengano emessi da ACM. AWS Questi certifica ti devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
Annex_I(1.3)	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Annex_I(1.3)	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindirizzi automaticamente le richieste HTTP non crittogra fate verso HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	api-gw-cache-enabled-and-encrypted	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per la cache della fase Gateway API. Per proteggere i dati sensibili che possono essere acquisiti per il metodo API, è necessario attivare la crittografia a riposo.
Annex_I(1.3)	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per contribuire a proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.
Annex_I(1.3)	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configurate con certificati SSL per consentire e ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.
Annex_I(1.3)	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.
Annex_I(1.3)	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
Annex_I(1.3)	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che vengano ruotate dopo aver raggiunto la fine del periodo di crittografia.
Annex_I(1.3)	backup-recovery-point-encrypted	Assicurati che la crittografia sia abilitata per i punti AWS di ripristino del Backup. Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
Annex_I(1.3)	codebuild-project-artifact-encryption	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CodeBuild artefatti.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	codebuild-project-s3-logs-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per AWS CodeBuild i log archiviati in Amazon S3.
Annex_I(1.3)	opensearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch Service.
Annex_I(1.3)	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
Annex_I(1.3)	opensearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittografia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	dynamodb-table-encrypted-kms	Assicurati che la crittografia sia abilitata per le tabelle Amazon DynamoDB. Data la possibile presenza di dati sensibili a riposo in queste tabelle, abilita la crittografia a riposo per proteggere tali dati. Per impostazione predefinita, le tabelle DynamoDB sono crittografate con AWS una chiave master del cliente (CMK) di proprietà.
Annex_I(1.3)	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
Annex_I(1.3)	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	elasticsearch-encrypted-at-rest	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi domini Amazon OpenSearch OpenSearch Service (Service).
Annex_I(1.3)	elasticsearch-node-to-node-encryption-check	Assicurati che node-to-node la crittografia per Amazon OpenSearch Service sia abilitata. ode-to-node La crittografia N abilita la crittogra fia TLS 1.2 per tutte le comunicazioni all'interno di Amazon Virtual Private Cloud (Amazon VPC). Poiché possono essere presenti dati sensibili, abilita la crittogra fia dei dati in transito per proteggere tali dati.
Annex_I(1.3)	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per protegger e i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribui re certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Annex_I(1.3)	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
Annex_I(1.3)	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (KMS).AWS Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	rds-snapshot-encrypted	Assicurati che la crittografia sia abilitata per gli snapshot Amazon Relational Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo, abilita la crittografia a riposo per proteggere tali dati.
Annex_I(1.3)	rds-storage-encrypted	Per aiutare a proteggere i dati a riposo, assicurati che la crittografia sia abilitata per le istanze Amazon Relationa l Database Service (Amazon RDS). Data la possibile presenza di dati sensibili a riposo nelle istanze Amazon RDS, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.
Annex_I(1.3)	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
Annex_I(1.3)	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
Annex_I(1.3)	sagemaker-endpoint-configuration-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo endpoint. SageMaker Poiché i dati sensibili possono esistere anche quando sono inattivi nell' SageMaker endpoint, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	sagemaker-notebook-instance-kms-key-configured	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo SageMaker notebook. Poiché i dati sensibili possono esistere anche quando sono inattivi nel SageMaker notebook, abilita la crittografia dei dati inattivi per proteggere tali dati.
Annex_I(1.3)	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.
Annex_I(1.3)	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantanee EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
Annex_I(1.3)	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicaz ione sicura tra il OpenSearch Servizio e altri servizi all'inter no di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.
Annex_I(1.3)	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principal i del cluster Amazon EMR possono contenere informazi oni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del AWS cloud. Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
Annex_I(1.3)	no-unrestricted-route-to-igw	Assicurati che le tabelle di routing di Amazon EC2 non abbiano percorsi illimitati verso un gateway Internet. La rimozione o la limitazione dell'accesso a Internet per i carichi di lavoro all'interno degli Amazon VPC può ridurre gli accessi non intenzionali all'interno del tuo ambiente.
Annex_I(1.3)	redshift-cluster-kms-enabled	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per il tuo cluster Amazon Redshift. Data la possibile presenza di dati sensibili a riposo nei cluster Redshift, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
Annex_I(1.3)	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicurando che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automatic amente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
Annex_I(1.3)	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
Annex_I(1.3)	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.
Annex_I(1.3)	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.
Annex_I(1.3)	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.
Annex_I(1.3)	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(1.3)	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
Annex_I(1.3)	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
Annex_I(5.1)	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(5.1)	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS
Annex_I(5.1)	waf-regional-rule-not-empty	Assicurati che il tuo AWS WAF abbia una regola che non sia vuota. Una regola senza condizioni può comportare un comportamento non intenzionale.
Annex_I(5.1)	waf-regional-rulegroup-not-empty	Assicurati che il tuo AWS WAF abbia un gruppo di regole che non sia vuoto. Un gruppo di regole vuoto potrebbe causare un comportamento indesiderato.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(5.1)	waf-regional-webacl-not-empty	Un ACL Web allegato a un AWS WAF può contenere una raccolta di regole e gruppi di regole per ispezionare e controllare le richieste Web. Se una ACL web è vuota, il traffico web passa senza essere rilevato o modificato dal WAF.
Annex_I(5.1)	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(5.1)	api-gw-associated-with-waf	AWS WAF ti consente di configurare una serie di regole (chiamate lista di controllo degli accessi Web (Web ACL)) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personali zzabili da te definite. La fase Gateway Amazon API deve essere associata a un ACL web WAF per garantire la protezione da attacchi dannosi.
Annex_I(5.1)	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(5.1)	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(6)	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.
Annex_I(6)	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(6)	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.
Annex_I(6)	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(6)	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(6)	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede l'impostazione di. allowVersionUpgrade Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.
Annex_I(6)	vuln-management-plan-exists (controllo del processo)	Assicurati che sia sviluppato e implementato un piano di gestione delle vulnerabilità in modo da disporre di processi formalmente definiti per affrontare le vulnerabilità nel tuo ambiente.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.1)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto» : «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazione dei compiti.
Annex_I(7.1)	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.1)	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.
Annex_I(7.1)	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.1)	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.2)	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti dichiarati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di Config	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
Annex_I(7.3)	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
Annex_I(7.4)	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.
Annex_I(7.4)	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.4)	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
Annex_I(7.4)	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.4)	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.
Annex_I(7.4)	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.4)	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.
Annex_I(7.4)	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.4)	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatch Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazioni dettagliate sul progetto di build.
Annex_I(7.4)	opensearch-audit-logging-enabled	Assicurati che la registrazione di controllo sia abilitata sui tuoi domini Amazon OpenSearch Service. La registrazione di controllo ti consente di tenere traccia delle attività degli utenti sui tuoi OpenSearch domini, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le query di OpenSearch ricerca in arrivo.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.4)	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori del servizio possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
Annex_I(7.4)	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.4)	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuat e le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED è abilitato . Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.4)	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurati che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.
Annex_I(7.4)	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisi zione dei record dettagliati relativi alle richieste effettuat e a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richieden te, nome del bucket, ora della richiesta, azione della richiesta , stato della risposta e codice di errore, se pertinente.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.4)	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
Annex_I(7.4)	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(7.4)	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.
Annex_I(10.2)	security-awareness-program-exists (controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organizzazione da eventuali violazioni della sicurezza o incidenti.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(12)	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.
Annex_I(12)	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(12)	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.
Annex_I(12)	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(12)	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
Annex_I(12)	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(12)	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfar e i requisiti di conformit à aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyV alue (Config default: 1), (requiredRetentionD ays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(12)	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.
Annex_I(12)	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(12)	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurat i che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.
Annex_I(12)	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	AWS Regola di Config	Linea guida
Annex_I(12)	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservar e più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'appl icazione e azioni non intenzion ali da parte degli utenti.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for RBI Cyber Security Framework for UCBs.

Best practice operative per RBI MD-ITF

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra il Master Direction — Information Technology Framework della Reserve Bank of India (RBI) e le regole AWS Config gestite. Ogni regola Config si applica a una AWS risorsa specifica e si riferisce a uno o più controlli RBI Master Direction — Information Technology Framework. Un controllo RBI Master Direction - Information Technology

Framework può essere correlato a più regole Config. Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(a)	Identificazione e classificazione delle risorse informative.	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
3.1(a)	Identificazione e classificazione delle risorse informative.	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2)

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			verificando se le istanze Amazon EC2 sono state interrott e per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.
3.1(a)	Identificazione e classificazione delle risorse informative.	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'eliminazione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata, potrebbe violare il concetto di funzionalità minima.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(a)	Identificazione e classificazione delle risorse informative.	ecr-private-tag-immutability-enabled	Abilita l'immutabilità dei tag di Elastic Container Repository (ECR) per evitare che i tag di immagine sulle immagini ECR vengano sovrascritti. In precedenza, i tag potevano essere sovrascritti, richiedendo metodologie manuali per identificare in modo univoco un'immagine.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
3.1(c)	Controllo accessi basato sui ruoli	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegi o minimo, assicurat i che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).
3.1(c)	Controllo accessi basato sui ruoli	efs-access-point-enforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitar e la gestione delle autorizzazioni e del privilegio minimo.
3.1(c)	Controllo accessi basato sui ruoli	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessari e. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(c)	Controllo accessi basato sui ruoli	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.
3.1(c)	Controllo accessi basato sui ruoli	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(g)	Gestione degli incidenti	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(g)	Gestione degli incidenti	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(g)	Gestione degli incidenti	alb-waf-enabled	Assicurati che AWS WAF sia abilitato su Elastic Load Balancers (ELB) per proteggere le applicazioni web. Un WAF aiuta a proteggere le applicazioni Web o le API contro gli exploit Web più comuni. Questi exploit Web possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive all'interno dell'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(g)	Gestione degli incidenti	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(g)	Gestione degli incidenti	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
3.1(h)	Trail	api-gw-execution-logging-enabled	La registrazione di log di Gateway API mostra viste dettagliate degli utenti che hanno effettuato l'accesso all'API e del modo in cui hanno effettuato l'accesso. Queste informazioni offrono visibilità sulle attività degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(h)	Trail	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attivit à degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'inter no del tuo Account AWS.
3.1(h)	Trail	codebuild-project-logging-enabled	Assicurati che la registrazione AWS CodeBuild del progetto sia abilitata in modo che i log di output della build vengano inviati ad Amazon o CloudWatc h Amazon Simple Storage Service (Amazon S3). I log di output della build forniscono informazi oni dettagliate sul progetto di build.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(h)	Trail	opensearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. OpenSearch I log degli errori dei servizi possono aiutare con i controlli di sicurezza e accesso e possono aiutare a diagnosticare problemi di disponibilità.
3.1(h)	Trail	redshift-audit-logging-enabled	Per acquisire informazioni sulle connessioni e sulle attività degli utenti nel tuo cluster Amazon Redshift, assicurati che la registrazione di log di audit sia abilitata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(h)	Trail	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio AWS registrando le azioni della Console di gestione e le chiamate API. È possibile identificare gli utenti e chi Account AWS ha chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
3.1(h)	Trail	cloudtrail-s3-dataevents-enabled	La raccolta di eventi di dati di Simple Storage Service (Amazon S3) aiuta a rilevare qualsiasi attività anomala. I dettagli includono Account AWS le informazioni relative all'accesso a un bucket Amazon S3, l'indirizzo IP e l'ora dell'evento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(h)	Trail	cw-loggroup-retention-period-check	Assicurati che i dati dei log degli eventi vengano mantenuti per una durata minima per i gruppi di log in modo da agevolare la risoluzione dei problemi e le indagini forensi. La mancata disponibilità dei dati dei log degli eventi passati rende difficile la ricostruzione e l'identificazione di eventi potenzialmente dannosi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(h)	Trail	elasticsearch-logs-to-cloudwatch	Assicurati che i domini OpenSearch di Amazon Service abbiano i log degli errori abilitati e trasmessi in streaming ad Amazon CloudWatch Logs per la conservazione e la risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(h)	Trail	elb-logging-enabled	L'attività di Elastic Load Balancing è un punto di comunicazione centrale all'interno di un ambiente. Assicurati che la registrazione di log di ELB sia abilitata. I dati raccolti forniscono informazioni dettagliate sulle richieste inviate a ELB. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(h)	Trail	multi-region-cloudtrail-enabled	AWS CloudTrail registra le azioni AWS della console di gestione e le chiamate API. È possibile identificare gli utenti e gli account chiamati AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. CloudTrail consegnerà i file di registro da tutte le AWS regioni al tuo bucket S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED è abilitato. Inoltre, quando AWS avvia una nuova regione, creerà lo stesso percorso nella nuova regione. CloudTrail Di conseguenza, riceverai file di log contenenti l'attività delle API per la nuova regione senza intraprendere alcuna azione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(h)	Trail	rds-logging-enabled	Per facilitare la registrazione di log e il monitoraggio nel tuo ambiente, assicurat i che la registrazione di log di Amazon Relational Database Service (Amazon RDS) sia abilitata. Con la registrazione di log di Amazon RDS, puoi acquisire eventi come connessioni, disconnessioni, query o tabelle interrogate.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(h)	Trail	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(h)	Trail	vpc-flow-logs-enabled	I log di flusso VPC forniscono record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(h)	Trail	wafv2-logging-enabled	Per facilitare la registrazione e il monitoraggio all'interno del tuo ambiente, abilita la registrazione AWS WAF (V2) sugli ACL web regionali e globali. AWS La registrazione WAF fornisce informazioni dettagliate sul traffico analizzato dall'ACL Web. I log registrano l'ora in cui AWS WAF ha ricevuto la richiesta dalla AWS risorsa, le informazioni sulla richiesta e un'azione per la regola corrispondente a ciascuna richiesta.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(h)	Trail	redshift-cluster-configuration-check	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i cluster Amazon Redshift. Devi inoltre verificare che le configurazioni richieste siano implementate sui cluster Amazon Redshift. La registrazione di log di audit deve essere abilitata per fornire informazioni su connessioni e attività degli utenti nel database. Questa regola richiede che sia impostato un valore per clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(i)	Infrastruttura a chiave pubblica	acm-certificate-expiration-check	Assicurati che l'integrità della rete sia protetta assicurando che i certificati X509 vengano emessi da ACM. AWS Questi certificati devono essere validi e non scaduti. Questa regola richiede un valore per daysToExpiration (valore AWS Foundational Security Best Practices: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
3.1(i)	Infrastruttura a chiave pubblica	alb-http-drop-invalid-header-enabled	Assicurati che i tuoi Elastic Load Balancer (ELB) siano configurati per eliminare le intestazioni http. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(i)	Infrastruttura a chiave pubblica	alb-http-to-https-redirection-check	Per proteggere i dati in transito, assicurati che l'Application Load Balancer reindiriz zi automaticamente le richieste HTTP non crittografate verso HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.
3.1(i)	Infrastruttura a chiave pubblica	api-gw-ssl-enabled	Assicurati che le fasi REST API del Gateway Amazon API siano configura te con certificati SSL per consentire ai sistemi di backend di autenticare la provenienza delle richieste dal Gateway API.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(i)	Infrastruttura a chiave pubblica	opensearch-https-required	Poiché possono esistere dati sensibili e per proteggere i dati in transito, assicurati che HTTPS sia abilitato per le connessioni ai tuoi domini Amazon OpenSearch Service.
3.1(i)	Infrastruttura a chiave pubblica	elbv2-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(i)	Infrastruttura a chiave pubblica	elb-acm-certificate-required	Per la possibile presenza di dati sensibili e per proteggere i dati in transito, assicurati che la crittografia sia abilitata per Elastic Load Balancing. Usa AWS Certificate Manager per gestire, fornire e distribuire certificati SSL/TLS pubblici e privati con AWS servizi e risorse interne.
3.1(i)	Infrastruttura a chiave pubblica	elb-tls-https-listeners-only	Assicurati che Elastic Load Balancer (ELB) sia configurato con ascoltatori SSL o HTTPS. Poiché possono essere presenti dati sensibili , abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.1(i)	Infrastruttura a chiave pubblica	redshift-require-tls-ssl	Assicurati che i cluster Amazon Redshift richiedano la crittografia TLS/SSL per connettersi ai client SQL. Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.
3.1(i)	Infrastruttura a chiave pubblica	s3-bucket-ssl-requests-only	Per aiutare a proteggere i dati in transito, assicurati che i bucket Amazon Simple Storage Service (Amazon S3) richiedano l'utilizzo di Secure Socket Layer (SSL). Poiché possono essere presenti dati sensibili, abilita la crittografia dei dati in transito per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Vulnerability Management	elastic-beanstalk-managed-updates-enabled	L'abilitazione degli aggiornamenti della piattaforma gestiti per un ambiente Amazon Elastic Beanstalk garantisce l'installazione degli ultimi aggiornamenti, correzioni e funzionalità disponibili per l'ambiente. Rimanere costantemente al passo con l'installazione delle patch è una delle best practice per la sicurezza dei sistemi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Vulnerability Management	rds-automatic-minor-version-upgrade-enabled	L'abilitazione degli aggiornamenti automatici delle versioni minori sulle istanze Amazon Relational Database Service (RDS) garantisce l'installazione degli ultimi aggiornamenti delle versioni minori del sistema di gestione di database relazionale (RDBMS), che possono includere patch di sicurezza e correzioni di bug.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Vulnerability Management	redshift-cluster-maintenancesettings-check	Questa regola garantisce che i cluster Amazon Redshift abbiano le impostazioni preferite per la tua organizzazione. In particolare, hanno finestre di manutenzione preferite e periodi di conservazione automatica degli snapshot per il database. Questa regola richiede di impostare il allowVersionUpgrade. Il valore predefinito è true. Inoltre, consente di impostare facoltativamente il preferredMaintenanceWindow (l'impostazione predefinita è sab: 16:00 -sab: 16:30) e il automatedSnapshotRetention periodo (l'impostazione predefinita è 1). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Vulnerability Management	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Vulnerability Management	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Vulnerability Management	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.3	Vulnerability Management	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5	Piano di gestione delle crisi informatiche	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5	Piano di gestione delle crisi informatiche	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5	Piano di gestione delle crisi informatiche	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5	Piano di gestione delle crisi informatiche	ec2-managedinstance-association-compliance-status-check	Utilizza AWS Systems Manager Associations per semplificare l'inventario delle piattaforme e delle applicazioni software all'interno di un'organizzazione. AWS Systems Manager assegna uno stato di configurazione alle istanze gestite e consente di impostare le linee di base dei livelli di patch del sistema operativo, delle installazioni software, delle configurazioni delle applicazioni e altri dettagli sull'ambiente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.5	Piano di gestione delle crisi informatiche	ec2-managedinstance-patch-compliance-status-check	L'abilitazione di questa regola facilita l'identificazione e la documentazione delle vulnerabilità Amazon Elastic Compute Cloud (Amazon EC2). La regola verifica se le istanze Amazon EC2 sono conformi alle patch in AWS Systems Manager, come richiesto dalle politiche e dalle procedure dell'organizzazione.
3.9	Valutazione del rischio IT	annual-risk-assessment-performed (controllo del processo)	Esegui una valutazione annuale del rischio sulla tua organizzazione. Le valutazioni del rischio possono aiutare a determinare la probabilità e l'impatto dei rischi e/o delle vulnerabilità identificati che interessano un'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
3.12	Addestramento	security-awareness -program-exists (controllo del processo)	Definizione e mantenimento di un programma di sensibilizzazione alla sicurezza per l'organizzazione. I programmi di sensibilizzazione alla sicurezza insegnano ai dipendenti come proteggere l'organiz zazione da eventuali violazioni della sicurezza o incidenti.
4.4(g)	Analisi delle frodi: analisi di transazioni sospette, appropria zione indebita, furto o sospetto riciclaggio di denaro, appropria zione indebita di beni, manipolazione di documenti finanziari e così via. L'obbligo normativo di segnalazi one delle frodi a RBI deve essere basato sul sistema.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	clb-multiple-az	Elastic Load Balancing (ELB) distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurati che ELB abbia registrato istanze da più zone di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuisce automatic amente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurat i che ELB abbia registrato istanze da più zone di disponibi lità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	lambda-vpc-multi-az-check	Se la tua funzione AWS Lambda è configurata per la connessione a un cloud privato virtuale (VPC) nel tuo account, implement a la funzione AWS Lambda in almeno due zone di disponibi lità diverse per assicurarti che sia disponibile per elaborare gli eventi in caso di interruzi one del servizio in una singola zona.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relational Database Service (Amazon RDS) offre disponibilità e durabilità avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automaticamente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibilità diversa. Ogni zona di disponibilità funziona su una propria infrastruttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infrastruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	s3-bucket-default-lock-enabled	Assicurati che il blocco sia abilitato, per impostazione predefinita, per il bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket S3, applica i blocchi degli oggetti a riposo per proteggere tali dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	vpc-vpn-2-tunnels-up	È possibile implement are tunnel VPN sito-sito ridondant i per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettiv ità nel caso in cui una delle connessio ni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessio ne VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	lambda-dlq-check	Abilita questa regola per avvisare il personale appropria to tramite Amazon Simple Queue Service (Amazon SQS) o Amazon Simple Notification Service (Amazon SNS) quando una funzione restituisce un errore.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	beanstalk-enhanced-health-reporting-enabled	AWS La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione. Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorare la disponibilità di Amazon RDS. Ciò fornisce una visibilità dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archiviazione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositivo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati, provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	ebs-optimized-instance	Un'istanza ottimizzata in Amazon Elastic Block Store (Amazon EBS) fornisce capacità dedicata aggiuntiva per le operazioni di I/O Amazon EBS. Tale ottimizzazione offre le prestazioni migliori in termini di efficienza per i volumi EBS, riducendo al minimo i conflitti tra le operazioni I/O Amazon EBS e altro traffico proveniente dall'istanza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(h)	Analisi della capacità e delle prestazioni dei sistemi di sicurezza IT.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(i)	Segnalazione degli incidenti, relativo impatto e misure adottate per evitare che tali eventi si ripetano in futuro.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
4.4(i)	Segnalazione degli incidenti, relativo impatto e misure adottate per evitare che tali eventi si ripetano in futuro.	guardduty-non-archived-findings	Amazon ti GuardDuty aiuta a comprendere l'impatto di un incidente classificando i risultati in base alla gravità: bassa, media e alta. Puoi utilizzare queste classificazioni per determinare le strategie e le priorità di correzione. Questa regola consente di impostare facoltativamente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) per i risultati non archiviati, come richiesto dalle politiche dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	aurora-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Aurora facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
6.3	Le NBFC prenderan no in considera zione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	backup-recovery-po int-minimum-retent ion-check	Per facilitare i processi di backup dei dati, assicurat i che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionD ays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'orga nizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	cmk-backing-key-rotation-enabled	Abilita la rotazione delle chiavi per assicurarti che le chiavi vengano ruotate dopo aver raggiunto la fine del periodo crittografico.
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	ec2-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tue risorse Amazon Elastic Compute Cloud (Amazon EC2) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatici possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	fsx-resources-protected-by-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon FSx facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
6.3	Le NBFC prenderanno in considerazione l'esigenza di creare i siti di backup necessari per i loro sistemi aziendali e data center critici.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	dynamodb-autoscaling-enabled	La scalabilità automatica di Amazon DynamoDB utilizza il servizio Application AWS Auto Scaling per regolare la capacità di throughput assegnata che risponde automaticamente ai modelli di traffico effettivi. In tal modo una tabella o un indice secondario globale può aumentare la capacità di lettura e scrittura assegnata per gestire improvvisi aumenti di traffico, senza alcuna limitazione (della larghezza di banda della rete).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	elb-cross-zone-load-balancing-enabled	Abilita il bilanciamento del carico tra zone per gli Elastic Load Balancer (ELB) per mantenere capacità e disponibilità adeguate. Il bilanciamento del carico tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata . Inoltre, migliora le capacità della tua applicazione di gestire la perdita di una o più istanze.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	elb-deletion-protection-enabled	Questa regola garantisce che per Elastic Load Balancing sia abilitata la protezione da eliminazione. Utilizza questa funzionalità per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	clb-multiple-az	Elastic Load Balancing (ELB) distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurati che ELB abbia registrato istanze da più zone di disponibilità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	elbv2-multiple-az	Elastic Load Balancing (ELB) distribuisce automatic amente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una zona di disponibilità. Per garantire un'elevata disponibilità, assicurat i che ELB abbia registrato istanze da più zone di disponibi lità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	lambda-vpc-multi-az-check	Se la tua funzione AWS Lambda è configurata per la connessione a un cloud privato virtuale (VPC) nel tuo account, implement a la funzione AWS Lambda in almeno due zone di disponibi lità diverse per assicurarti che sia disponibile per elaborare gli eventi in caso di interruzi one del servizio in una singola zona.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	rds-instance-deletion-protection-enabled	Assicurati che per le istanze di Amazon Relationa l Database Service (Amazon RDS) sia abilitata la protezion e da eliminazione. Utilizza la protezion e da eliminazione per evitare che le istanze Amazon RDS vengano eliminate accidentalmente o intenzionalmente, con conseguente perdita di disponibilità delle applicazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	rds-multi-az-support	Il supporto multi-AZ in Amazon Relationa l Database Service (Amazon RDS) offre disponibilità e durabilit à avanzate per le istanze database. Quando esegui il provisioning di un'istanza database multi-AZ, Amazon RDS crea automatic amente un'istanza database primaria e replica in modo sincrono i dati in un'istanza standby in una zona di disponibi lità diversa. Ogni zona di disponibi lità funziona su una propria infrastru ttura indipendente e fisicamente distinta ed è progettata per essere altamente affidabile. In caso di guasto dell'infr astruttura, Amazon RDS esegue un failover automatico in standby in modo da poter riprender

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e le operazioni del database non appena il failover è completato.
8.1	I sistemi IT devono essere progressivamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	vpc-vpn-2-tunnels-up	È possibile implementare tunnel VPN sito-sito ridondanti per soddisfare i requisiti di resilienza. Utilizza due tunnel per garantire la connettività nel caso in cui una delle connessioni VPN sito-sito non sia disponibile. Per evitare la perdita di connettività nel caso in cui il gateway del cliente non sia più disponibile, puoi configurare una seconda connessione VPN sito-sito al tuo Amazon Virtual Private Cloud (Amazon VPC) e al gateway privato virtuale utilizzando un secondo dispositivo gateway del cliente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	autoscaling-group-elb-healthcheck-required	I controlli dell'integrità Elastic Load Balancer (ELB) per i gruppi con dimensionamento automatico Amazon Elastic Compute Cloud (Amazon EC2) supportan o il mantenime nto di capacità e disponibilità adeguate. Periodicamente, il sistema di bilanciam ento del carico invia ping, effettua tentativi di connessione o invia richieste per testare lo stato delle istanze Amazon EC2 in un gruppo con dimension amento automatic o. Se un'istanza non risponde, il traffico viene inviato a una nuova istanza Amazon EC2.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	dynamodb-throughput-limit-check	Abilita questa regola per assicurarti che la capacità effettiva di trasmissione assegnata sia verificata nelle tabelle Amazon DynamoDB. Questa è la quantità di attività di lettura e scrittura che ogni tabella può supportare. DynamoDB utilizza queste informazioni per prenotare risorse di sistema sufficienti per soddisfare le esigenze di velocità effettiva. Questa regola genera un avviso quando la velocità di trasmissione effettiva si avvicina al limite massimo per l'account di un cliente. Questa regola consente di impostare facoltativamente i parametri AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			(Config Default: 80). I valori effettivi devono riflettere le policy dell'organizzazione.
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitorag gio relativi all'istanza a intervalli di 1 minuto.
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informati ca utilizzando i feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendimento automatico per identificare attività impreviste, non autorizzate e dannose all'interno del tuo AWS ambiente cloud.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	lambda-concurrency-check	Questa regola garantisce che vengano stabiliti i limiti massimi e minimi di simultaneità di una funzione Lambda. Ciò può aiutare a stabilire il numero di richieste che la funzione serve in un dato momento.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	rds-enhanced-monitoring-enabled	Abilita Amazon Relational Database Service (Amazon RDS) per monitorar e la disponibilità di Amazon RDS. Ciò fornisce una visibilit à dettagliata sullo stato delle istanze database Amazon RDS. Quando l'archivi azione di Amazon RDS utilizza più di un dispositivo fisico sottostante, Enhanced Monitoring raccoglie i dati per ogni dispositi vo. Inoltre, quando l'istanza database Amazon RDS è in esecuzione in una implementazione multi-AZ, vengono raccolti i dati per ogni dispositivo sull'host secondario e le metriche dell'host secondario.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.1	I sistemi IT devono essere progressi vamente aumentati man mano che aumentano le dimensioni e la complessità delle operazioni delle NBFC.	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessio ni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check . Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	dms-replication-not-public	Gestisci l'accesso al AWS cloud assicurando che le istanze di replica DMS non siano accessibili pubblicamente. Le istanze di replica DMS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	ebs-snapshot-public-restorable-check	Gestisci l'accesso al AWS cloud assicurandoti che le istantane e EBS non siano ripristinabili pubblicamente. Gli snapshot dei volumi EBS possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze di Amazon Elastic Compute Cloud (Amazon EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	elasticsearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini Amazon OpenSearch Service (OpenSearch Service) si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio di OpenSearch servizio all'interno di un Amazon VPC consente una comunicazione sicura tra il OpenSearch Servizio e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	emr-master-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che i nodi master del cluster Amazon EMR non siano accessibili pubblicamente. I nodi principali del cluster Amazon EMR possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'inter no di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicaz ione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configura zione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttamente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	rds-instance-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	rds-snapshots-public-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che le istanze di Amazon Relational Database Service (Amazon RDS) non siano pubbliche. Le istanze database Amazon RDS possono contenere informazi oni e principi sensibili e per tali account è necessario il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/logici e una policy sulle password ben definita.	redshift-cluster-public-access-check	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che i cluster Amazon Redshift non siano pubblici. I cluster Amazon Redshift possono contenere informazioni e principi sensibili e per tali account è necessari o il controllo degli accessi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/logici e una policy sulle password ben definita.	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/logici e una policy sulle password ben definita.	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	s3-bucket-public-read-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	s3-bucket-public-write-prohibited	Gestisci l'accesso alle risorse nel AWS cloud permettendo solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	sagemaker-notebook-no-direct-internet-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che SageMaker i notebook Amazon non consentano l'accesso diretto a Internet. Impedendo l'accesso diretto a Internet, puoi impedire l'accesso ai dati sensibili da parte di utenti non autorizzati.
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'acce sso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefini to aiuta a limitare l'accesso remoto alle risorse. AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'acce sso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integ rità e alla riservate zza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controlla re l'accesso remoto a sistemi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/logici e una policy sulle password ben definita.	access-keys-rotated	Le credenziali vengono verificate per dispositivi, utenti e processi autorizzati assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza. Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configurazione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	emr-kerberos-enabled	I permessi e le autorizzazioni di accesso possono essere gestiti e incorporati con i principi del privilegi o minimo e della separazione dei compiti, abilitand o Kerberos per i cluster Amazon EMR. In Kerberos, i servizi e gli utenti che devono effettuar e l'autenticazione sono denominati principali. I principali si trovano in un realm Kerberos. All'interno del realm, un server Kerberos è noto come centro di distribuz ione delle chiavi (KDC). Fornisce un mezzo per l'autenti cazione dei principal i. Il KDC effettua l'autenticazione emettendo dei ticket. Il KDC gestisce un database dei principali nel realm, le relative password

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			e altre informazioni amministrative su ogni principale.
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/logici e una policy sulle password ben definita.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	autoscaling-launch-config-public-ip-disabled	Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete sono raggiungibili da Internet. Le risorse EC2 non devono essere accessibili pubblicamente, in quanto ciò può consentire un accesso non intenzionale alle applicazioni o ai server.
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associazione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	ecs-task-definition-nonroot-user	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che un utente non root sia designato per l'accesso alle definizioni delle attività Amazon Elastic Container Service (Amazon ECS).

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/logici e una policy sulle password ben definita.	efs-access-point-enforce-root-directory	L'applicazione di una directory root per un punto di accesso Amazon Elastic File System (Amazon EFS) aiuta a limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano raggiungere solo i file della sottodirectory specificata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/logici e una policy sulle password ben definita.	efs-access-point-enforce-user-identity	Per facilitare l'implementazione del principio del privilegio minimo, assicurati che l'applicazione dell'utente sia abilitata per il tuo Amazon Elastic File System (Amazon EFS). Quando è abilitato, Amazon EFS sostituisce gli ID utente e gruppo del client NFS con l'identità configurata sul punto di accesso per tutte le operazioni sul file system e concede l'accesso solo a questa identità utente applicata.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/logici e una policy sulle password ben definita.	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanismi di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consigliabile utilizzare le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	subnet-auto-assign-public-ip-disabled	Gestisci l'accesso al AWS cloud assicuran do che alle sottoreti Amazon Virtual Private Cloud (VPC) non venga assegnato automaticamente un indirizzo IP pubblico. Le istanze Amazon Elastic Compute Cloud (EC2) lanciate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato all'interfaccia di rete principale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/logici e una policy sulle password ben definita.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controllato controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel AWS cloud. Questa regola garantisce che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/logici e una policy sulle password ben definita.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Management (IAM) che dispongon o di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezion e alle credenziali di accesso. Richiedendo agli utenti di effettuar e l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/logici e una policy sulle password ben definita.	opensearch-in-vpc-only	Gestisci l'accesso al AWS cloud assicurandoti che i domini di Amazon OpenSearch Service si trovino all'interno di un Amazon Virtual Private Cloud (Amazon VPC). Un dominio Amazon OpenSearch Service all'interno di un Amazon VPC consente una comunicazione sicura tra Amazon OpenSearch Service e altri servizi all'interno di Amazon VPC senza la necessità di un gateway Internet, un dispositivo NAT o una connessione VPN.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.
8.I	Aspetti di sicurezza di base come i controlli degli accessi fisici/ logici e una policy sulle password ben definita.	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.II	Un ruolo utente ben definito.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizzazioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativ a è un modo per incorporare il privilegi o minimo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.II	Un ruolo utente ben definito.	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Managemen t) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzar e politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizz abilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizzazioni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.II	Un ruolo utente ben definito.	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica sulle password. I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.II	Un ruolo utente ben definito.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizzazioni di accesso, impedendo alle policy di contenere «Effetto»: «Consenti» con «Azione»: «*» rispetto a «Resource»: «*». Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.II	Un ruolo utente ben definito.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
8.II	Un ruolo utente ben definito.	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibilità che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.II	Un ruolo utente ben definito.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.III	Un concetto maker-checker per ridurre il rischio di errori e usi impropri e per assicurare l'affidabilità dei dati/delle informazioni.	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.IX	Disposizione per il backup dei dati con test periodici.	db-instance-backup-enabled	La funzionalità di backup di Amazon RDS crea backup dei database e dei log delle transazioni. Amazon RDS crea automaticamente uno snapshot di archiviazione del volume dell'istanza database, eseguendo il backup dell'intera istanza. Il sistema consente di impostare periodi di conservazione specifici per soddisfare i requisiti di resilienza.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.IX	Disposizione per il backup dei dati con test periodici.	dynamodb-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le tabelle Amazon DynamoDB facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.IX	Disposizione per il backup dei dati con test periodici.	dynamodb-pitr-enabled	Abilita questa regola per verificare che sia stato eseguito il backup delle informazioni. Inoltre, mantiene i backup assicurando che il point-in-time ripristino sia abilitato in Amazon DynamoDB. Il ripristino mantiene i backup continui della tabella degli ultimi 35 giorni.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.IX	Disposizione per il backup dei dati con test periodici.	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.IX	Disposizione per il backup dei dati con test periodici.	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.IX	Disposizione per il backup dei dati con test periodici.	elasticache-redis-cluster-automatic-backup-check	Quando i backup automatici sono abilitati, Amazon ElastiCache crea un backup del cluster su base giornaliera. Il backup può essere mantenuto per un certo numero di giorni, come specificato dall'organizzazione. I backup automatic i possono fornire protezione da perdita di dati. Se si verifica un errore, puoi creare un nuovo cluster, che ripristina i dati dal backup più recente.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.IX	Disposizione per il backup dei dati con test periodici.	rds-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che le istanze di Amazon Relational Database Service (Amazon RDS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completam ente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.IX	Disposizione per il backup dei dati con test periodici.	s3-bucket-replication-enabled	La replica tra regioni (CRR) di Amazon Simple Storage Service (Amazon S3) supporta il mantenimento di capacità e disponibilità adeguate. La replica tra regioni (CRR) consente la copia asincrona e automatica di oggetti tra bucket Amazon S3 per assicurare il mantenimento della disponibilità dei dati.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.IX	Disposizione per il backup dei dati con test periodici.	redshift-backup-enabled	Per facilitare i processi di backup dei dati, assicurati che i cluster Amazon Redshift dispongano di snapshot automatizzati. Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Redshift scatta un'istantanea ogni otto ore o ogni 5 GB per ogni nodo di modifica dei dati o per qualsiasi evento che si verifica per primo.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.IX	Disposizione per il backup dei dati con test periodici.	backup-plan-min-frequency-and-min-retention-check	Per facilitare i processi di backup dei dati, assicurati che il piano di AWS Backup sia impostato per una frequenza e una conservazione minime. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare i parametri requiredFrequencyValue (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). Il valore effettivo deve essere conforme ai

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
			requisiti dell'orga nizzazione.
8.IX	Disposizione per il backup dei dati con test periodici.	backup-recovery-point-manual-deletion-disabled	Assicurati che ai punti AWS di ripristino di Backup sia associata una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino. L'utilizzo di una policy basata sulle risorse che impedisca l'elimina zione dei punti di ripristino può aiutare a prevenire l'elimina zione accidentale o intenzionale.

ID controllo	Descrizione del controllo	AWS Regola di Config	Linea guida
8.IX	Disposizione per il backup dei dati con test periodici.	backup-recovery-point-minimum-retention-check	Per facilitare i processi di backup dei dati, assicurati che per i punti di ripristino di AWS Backup sia impostato un periodo minimo di conservazione. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup. Questa regola consente di impostare il parametro requiredRetentionDays (configurazione predefinita: 35). Il valore effettivo deve essere conforme ai requisiti dell'organizzazione.

Modello

Il modello è disponibile su GitHub: Operational Best Practices for RBI MD-ITF.

Best practice operative per servizi di sicurezza, identità e conformità

Questo pacchetto di conformità contiene AWS Config regole basate sui servizi di sicurezza, identità e conformità. Per ulteriori informazioni, consulta Sicurezza, identità e conformità su. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Security, Identity and Compliance Services.

Best practice operative per serverless

Questo pacchetto di conformità contiene AWS Config regole basate su soluzioni serverless. Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle AWS Config regole gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Serverless.

Best practice operative per servizi di archiviazione

Questo pacchetto di conformità contiene AWS Config regole basate su Storage Services. Per ulteriori informazioni, consulta Cloud Storage on. AWS Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Operational Best Practices for Storage Services.

Best practice operative per SWIFT CSP

I Conformance Pack forniscono un framework di conformità generico progettato per consentire di creare controlli di governance relativi alla sicurezza, all'operatività o all'ottimizzazione dei costi utilizzando regole gestite o personalizzate e azioni correttive. AWS Config AWS Config I pacchetti di conformità, in quanto modelli di esempio, non sono pensati per garantire la piena conformità a uno specifico standard di governance o conformità. È tua responsabilità valutare autonomamente se l'utilizzo dei Servizi soddisfa i requisiti legali e normativi applicabili.

Di seguito viene fornito un esempio di mappatura tra SWIFT Customer Security Programme (CSP) e le regole AWS Config gestite. Ogni AWS Config regola si applica a una AWS risorsa specifica e si riferisce a uno o più controlli SWIFT CSP. Un controllo SWIFT CSP può essere correlato a più regole. AWS Config Consulta la tabella seguente per maggiori dettagli e indicazioni relativi a queste mappature.

ID controllo	AWS Regola di configurazione	Linea guida
1.1	ec2-instance-managed-by-systems-manager	Un inventario delle piattaforme software e delle applicazioni all'interno dell'organizzazione è possibile gestendo le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager. AWS Utilizzate AWS Systems Manager per fornire configurazioni di sistema dettagliate, livelli di patch del sistema operativo, nome e tipo di servizi, installazioni software, nome dell'applicazione, editore e versione e altri dettagli sull'ambiente.
1.1	ec2-instance-no-public-ip	Gestisci l'accesso al AWS cloud assicurando che le istanze Amazon Elastic Compute Cloud (Amazon

ID controllo	AWS Regola di configurazione	Linea guida
		EC2) non siano accessibili pubblicamente. Le istanze Amazon EC2 possono contenere informazioni sensibili e per tali account è necessario il controllo degli accessi.
1.1	ec2-no-amazon-key-pair	Questa regola verifica se le istanze Amazon Elastic Compute Cloud (Amazon EC2) in esecuzione vengono avviate tramite le coppie di chiavi Amazon. Questo può aiutare a ridurre il rischio di compromissione delle credenziali. È ancora possibile accedere alle istanze Amazon EC2 senza coppie di chiavi utilizzando Session Manager o una connessione SSH basata su browser tramite la console. AWS

ID controllo	AWS Regola di configurazione	Linea guida
1.1	ec2-instances-in-vpc	Implementa istanze Amazon Elastic Compute Cloud (Amazon EC2) in un Amazon Virtual Private Cloud (Amazon VPC) per abilitare la comunicazione sicura tra un'istanza e altri servizi all'interno di Amazon VPC, senza la necessità di un gateway Internet, un dispositi vo NAT o una connessione VPN. Tutto il traffico rimane sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Assegna istanze Amazon EC2 a un Amazon VPC per gestire correttamente l'accesso.

ID controllo	AWS Regola di configurazione	Linea guida
1.1	vpc-default-security-group-closed	I gruppi di sicurezza di Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare nella gestione dell'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Limitare tutto il traffico sul gruppo di sicurezza predefinito aiuta a limitare l'accesso remoto alle risorse. AWS
1.1	vpc-network-acl-unused-check	Questa regola garantisce che le liste di controllo degli accessi di rete del cloud privato virtuale (VPC) di Amazon siano in uso. Il monitoraggio delle liste di controllo degli accessi di rete non utilizzati può aiutare a effettuare un inventario e una gestione accurati del proprio ambiente.

ID controllo	AWS Regola di configurazione	Linea guida
1.1	vpc-sg-open-only-to-authorized-ports	Gestisci l'accesso alle risorse nel AWS cloud assicurando che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazione dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Limitando l'accesso alle risorse in un gruppo di sicurezza da Internet (0.0.0.0/0) è possibile controllare l'accesso remoto a sistemi interni.

ID controllo	AWS Regola di configurazione	Linea guida
1.2	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con permessi e autorizza zioni di accesso, impedendo alle policy di contenere azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. Avere più privilegi del necessario per completare un'attività può violare il principio del privilegi o minimo e della separazio ne dei compiti. Questa regola consente di impostare il parametro. blockedActionsPatt erns (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
1.2	iam-group-has-users-check	AWS Identity and Access Management (IAM) può aiutarti a incorporare i principi del privilegio minimo e della separazione dei compiti con i permessi e le autorizza zioni di accesso, assicuran do che i gruppi IAM abbiano almeno un utente. Collocare gli utenti in gruppi in base ai permessi associati o alla funzione lavorativa è un modo per incorporare il privilegio minimo.

ID controllo	AWS Regola di configurazione	Linea guida
1.2	iam-inline-policy-blocked-kms-actions	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per consentire azioni bloccate su AWS tutte le chiavi del servizio di gestione delle chiavi. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni. Questa regola consente di impostare il blockedAc tionsPatterns parametro. (Valore delle migliori pratiche di sicurezza di AWS base: kms:Decrypt, kms: From). ReEncrypt I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
1.2	iam-no-inline-policy-check	Assicurati che un utente, un ruolo IAM o un gruppo IAM (AWS Identity and Access Management) non disponga di una policy in linea per controllare l'accesso a sistemi e asset. AWS consiglia di utilizzare politiche gestite anziché politiche in linea. Le policy gestite consentono la riutilizzabilità, il controllo delle versioni, il rollback e la delega della gestione delle autorizza zioni.
1.2	iam-user-no-policies-check	Questa regola garantisce che le policy di AWS Identity and Access Management (IAM) siano collegate solo a gruppi o ruoli per controllare l'accesso a sistemi e asset. L'assegnazione di privilegi a livello di gruppo o di ruolo aiuta a ridurre le possibili tà che un'identità riceva o mantenga privilegi eccessivi.

ID controllo	AWS Regola di configurazione	Linea guida
1.2	restricted-ssh	I gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) possono aiutare a gestire l'accesso alla rete fornendo un filtro stateful del traffico di rete in ingresso e in uscita verso le risorse. AWS Non consentire il traffico in entrata (o remoto) da 0.0.0.0/0 alla porta 22 sulle risorse contribuisce a limitare l'accesso remoto.
1.2	nacl-no-unrestricted-ssh-rdp	Le porte di amministrazione del server remoto nelle liste di controllo degli accessi alla rete (ACL), come la porta 22 (SSH) e la porta 3389 (RDP), non devono essere accessibi li pubblicamente, in quanto ciò potrebbe comportare l'accesso indesiderato alle risorse nel VPC.

ID controllo	AWS Regola di configurazione	Linea guida
1.2	s3-bucket-acl-prohibited	Questa regola verifica se le liste di controllo degli accessi (ACL) vengono utilizzate per il controllo degli accessi ai bucket Amazon S3. Gli ACL sono meccanismi di controllo degli accessi legacy per i bucket Amazon S3 AWS precedenti a Identity and Access Management (IAM). Invece delle ACL, è consiglia bile utilizzare le policy IAM o le policy dei bucket S3 per gestire più facilmente l'accesso ai bucket S3.

ID controllo	AWS Regola di configurazione	Linea guida
1.2	s3-bucket-logging-enabled	La registrazione di log degli accessi al server Amazon Simple Storage Service (Amazon S3) è un metodo per monitorare la rete a fronte di potenziali eventi di cibersicurezza. Gli eventi sono monitorati mediante l'acquisizione dei record dettagliati relativi alle richieste effettuate a un bucket Amazon S3. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso. I dettagli includono richiedente, nome del bucket, ora della richiesta, azione della richiesta, stato della risposta e codice di errore, se pertinente.
1.2	s3-bucket-policy-grantee-check	Gestisci l'accesso al AWS cloud abilitando s3_ bucket_policy_grantee_check. Questa regola verifica che l'accesso concesso dal bucket Amazon S3 sia limitato dai AWS principali, dagli utenti federati, dai responsabili del servizio, dagli indirizzi IP o dagli ID Amazon Virtual Private Cloud (Amazon VPC) forniti.

ID controllo	AWS Regola di configurazione	Linea guida
1.2	sns-topic-message-delivery-notification-enabled	Per semplificare i requisiti di registrazione nell'ambiente, assicurati che le notifiche sullo stato di consegna siano abilitate per gli argomenti Amazon Simple Notificat ion Service (Amazon SNS). La registrazione dello stato di consegna dei messaggi aiuta a ottenere informazioni operative migliori, ad esempio sapere se un messaggio è stato consegnato all'endpo int Amazon SNS, identificare la risposta inviata dall'endp oint Amazon SNS ad Amazon SNS e determinare il tempo di attesa del messaggio (il periodo di tempo tra il timestamp di pubblicazione e l'istante immediatamente precedente alla consegna a un endpoint Amazon SNS).

ID controllo	AWS Regola di configurazione	Linea guida
1.4	internet-gateway-authorized-vpc-only	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che i gateway Internet siano collegati solo a Amazon Virtual Private Cloud (Amazon VPC) autorizzato. I gateway Internet consentono l'accesso bidirezionale a Internet da e verso Amazon VPC, il che può potenzialmente portare all'accesso non autorizzato alle risorse Amazon VPC.
1.4	restricted-common-ports	Gestisci l'accesso alle risorse nel AWS cloud assicuran do che le porte comuni siano limitate sui gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2). La mancata limitazio ne dell'accesso alle porte a origini attendibili può essere causa di attacchi alla disponibilità, all'integrità e alla riservatezza dei sistemi. Questa regola consente di impostare facoltativamente i parametri blockedPort1 - blockedPort5 (valori di configurazione predefiniti: 20,21,3389,3306,4333). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
1.4	lambda-function-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS Cloud assicurando che le funzioni AWS Lambda non siano accessibili pubblicamente. L'accesso pubblico può comportare una riduzione della disponibilità delle risorse.
1.4	s3-account-level-public-access-blocks-periodic	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibili pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico. Questa regola consente di impostare facoltativamente (Config Default: True), ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True) e i restrictPublicBuckets parametri blockPublicAcls (Config Default: True). I valori effettivi devono riflettere le policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
1.4	s3-bucket-level-public-access-prohibited	Gestisci l'accesso alle risorse nel AWS cloud assicurando che i bucket Amazon Simple Storage Service (Amazon S3) non siano accessibi li pubblicamente. Questa regola aiuta a proteggere i dati sensibili da utenti remoti non autorizzati impedendo l'accesso pubblico a livello di bucket.
1.4	s3-bucket-public-read-prohi bited	Gestisci l'accesso alle risorse nel AWS cloud permetten do solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.
1.4	s3-bucket-public-write-proh ibited	Gestisci l'accesso alle risorse nel AWS cloud permetten do solo a utenti, processi e dispositivi autorizzati di accedere ai bucket Amazon Simple Storage Service (Amazon S3). La gestione dell'accesso deve essere coerente con la classificazione dei dati.

ID controllo	AWS Regola di configurazione	Linea guida
1.4	ssm-document-not-public	Assicurati che AWS i documenti di Systems Manager (SSM) non siano pubblici, in quanto ciò potrebbe consentire l'accesso non intenzionale ai tuoi documenti SSM. Un documento SSM pubblico può esporre informazioni su account, risorse e processi interni.
2.3	ec2-imdsv2-check	Assicurati che il metodo del servizio di metadati di istanza versione 2 (IMDSv2) sia abilitato per protegger e l'accesso e il controllo dei metadati delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Il metodo IMDSv2 utilizza controlli basati sulla sessione. Con IMDSv2, puoi implementare controlli per limitare le modifiche ai metadati delle istanze.

ID controllo	AWS Regola di configurazione	Linea guida
2.3	ec2-instance-multiple-eni-check	Questa regola verifica se le istanze Amazon Elastic Compute Cloud (Amazon EC2) hanno più ENI. La presenza di più ENI può causare istanze dual-homed, ovvero istanze con più sottoreti. Ciò può aumentare la complessità della sicurezza della rete e introdurre percorsi e accessi di rete indesiderati.
2.3	ec2-token-hop-limit-check	Assicurati che la risposta HTTP PUT del servizio di metadati di istanza (IMDS) sia limitata all'istanza Amazon Elastic Compute Cloud (Amazon EC2). Con IMDSv2, la risposta PUT che contiene il token segreto per impostazione predefinita non può uscire dall'istanza, poiché il limite di hop di risposta dei metadati è impostato su 1 (valore di configurazione predefinito). Se questo valore è maggiore di 1, il token può lasciare l'istanza EC2.

ID controllo	AWS Regola di configurazione	Linea guida
2.3	ec2-volume-inuse-check	Questa regola garantisce che i volumi Amazon Elastic Block Store collegati a istanze Amazon Elastic Compute Cloud (Amazon EC2) siano contrassegnati per l'elimina zione quando un'istanza viene terminata. Se un volume Amazon EBS non viene eliminato quando l'istanza a cui è collegato viene terminata , potrebbe violare il concetto di funzionalità minima.
2.3	account-part-of-organizations	La gestione centralizzata Account AWS all'interno di AWS Organizations aiuta a garantire la conformità degli account. L'assenza di una governance centralizzata degli account può comportar e configurazioni incoerenti di account, il che può mettere a rischio risorse e dati sensibili.

ID controllo	AWS Regola di configurazione	Linea guida
2.3	lambda-inside-vpc	Implementa le funzioni AWS Lambda all'interno di un Amazon Virtual Private Cloud (Amazon VPC) per una comunicazione sicura tra una funzione e altri servizi all'interno di Amazon VPC. Questa configurazione non richiede un gateway Internet, un dispositivo NAT o una connessione VPN. Tutto il traffico rimane in modo sicuro all'interno del cloud. AWS Grazie all'isolamento logico, i domini che si trovano all'interno di un Amazon VPC hanno un ulteriore livello di sicurezza rispetto ai domini che usano gli endpoint pubblici. Per gestire correttam ente l'accesso, le funzioni AWS Lambda devono essere assegnate a un VPC.

ID controllo	AWS Regola di configurazione	Linea guida
2.3	kms-cmk-not-scheduled-for-deletion	Per proteggere i dati archiviati, assicurati che non sia pianificata l'eliminazione delle chiavi master del cliente (CMK) necessarie nel AWS Key Management Service (AWS KMS). Poiché a volte l'eliminazione delle chiavi è necessaria, questa regola può aiutare a verificare tutte le chiavi per le quali è pianificata l'eliminazione, nel caso in cui una chiave sia stata pianificata in modo non intenzionale.
2.3	s3-bucket-versioning-enabled	Il controllo delle versioni del bucket Amazon Simple Storage Service (Amazon S3) consente di conservare più varianti di un oggetto nello stesso bucket Amazon S3. Utilizza il controllo delle versioni per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni agevola il ripristino a seguito di errori dell'applicazione e azioni non intenzionali da parte degli utenti.

ID controllo	AWS Regola di configurazione	Linea guida
2.3	secretsmanager-secret-unused	Se in AWS Secrets Manager sono presenti credenziali inutilizzate, è necessario disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola consente di impostare un valore su unusedForDays (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.
2.5A	ebs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i volumi Amazon Elastic Block Store (Amazon EBS) facciano parte di un piano di backup. AWS AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplifica la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
2.5A	ec2-ebs-encryption-by-default	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS). Data la possibile presenza di dati sensibili a riposo in questi volumi, abilita la crittografia a riposo per proteggere tali dati.
2.5A	efs-encrypted-check	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per Amazon Elastic File System (EFS).
2.5A	efs-in-backup-plan	Per facilitare i processi di backup dei dati, assicurati che i tuoi file system Amazon Elastic File System (Amazon EFS) facciano parte di un piano di AWS backup. AWS Backup è un servizio di backup completamente gestito con una soluzione di backup basata su policy. Questa soluzione semplific a la gestione dei backup e consente di soddisfare i requisiti di conformità aziendali e normativi in materia di backup.

ID controllo	AWS Regola di configurazione	Linea guida
2.5A	encrypted-volumes	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i volumi Amazon Elastic Block Store (Amazon EBS).
2.5A	kinesis-stream-encrypted	Data la possibile presenza di dati sensibili e per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i flussi di Amazon Kinesis.
2.5A	s3-bucket-server-side-encryption-enabled	Per proteggere i dati a riposo, assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo nei bucket Amazon S3, abilita la crittografia per proteggere tali dati.
2.5A	s3-default-encryption-kms	Assicurati che la crittografia sia abilitata per i bucket Amazon Simple Storage Service (Amazon S3). Data la possibile presenza di dati sensibili a riposo in un bucket Amazon S3, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
2.5A	sns-encrypted-kms	Per proteggere i dati archiviati, assicurati che gli argomenti di Amazon Simple Notification Service (Amazon SNS) richiedano la crittografia AWS tramite Key Management Service AWS (KMS). Data la possibile presenza di dati sensibili a riposo nei messaggi pubblicati, abilita la crittografia a riposo per proteggere tali dati.

ID controllo	AWS Regola di configurazione	Linea guida
4.1	iam-password-policy	Le identità e le credenziali vengono emesse, gestite e verificate in base a una policy IAM sulle password dell'organizzazione. Soddisfano o superano i requisiti indicati dal NIST SP 800-63 e dallo standard AWS Foundational Security Best Practices per la sicurezza delle password. Questa regola consente di impostare facoltativamente RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24) e MaxPasswordAge (AWS Foundational Security Best Practices value: 90) per il tuo IAM Politica in materia

ID controllo	AWS Regola di configurazione	Linea guida
		di password. I valori effettivi devono riflettere le policy dell'organizzazione.
4.1	access-keys-rotated	Le credenziali vengono verificate per i dispositivi, gli utenti e i processi autorizza ti assicurando che le chiavi di accesso IAM vengano ruotate come specificato dalla politica organizzativa. La modifica delle chiavi di accesso a intervalli regolari è una best practice di sicurezza . Riduce il periodo di attività di una chiave di accesso e l'impatto aziendale in caso di compromissione delle chiavi. Questa regola richiede un valore di rotazione delle chiavi di accesso (valore di configura zione predefinito: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
4.2	iam-user-mfa-enabled	Abilita questa regola per limitare l'accesso alle risorse nel cloud. AWS Questa regola garantisce che l'autenti cazione a più fattori (MFA) sia abilitata per tutti gli utenti. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Riduci gli incidenti dovuti alla compromissione degli account richiedendo l'autenticazione a più fattori per gli utenti.
4.2	mfa-enabled-for-iam-console-access	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per tutti gli utenti di AWS Identity and Access Managemen t (IAM) che dispongono di una password di console. La tecnologia MFA aggiunge un ulteriore livello di protezione alle credenziali di accesso. Richiedendo agli utenti di effettuare l'autenticazione a più fattori, puoi ridurre gli incidenti dovuti alla compromis sione degli account e impedire l'accesso ai dati sensibili agli utenti non autorizzati.

ID controllo	AWS Regola di configurazione	Linea guida
4.2	root-account-hardware-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che la MFA hardware sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS
4.2	root-account-mfa-enabled	Gestisci l'accesso alle risorse nel AWS cloud assicurandoti che l'MFA sia abilitata per l'utente root. L'utente root è l'utente più privilegiato in un Account AWS. L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione per le credenziali di accesso. Richiedendo l'MFA per l'utente root, è possibile ridurre i casi di compromissione. Account AWS

ID controllo	AWS Regola di configurazione	Linea guida
5.1	ec2-instance-profile-attached	I profili dell'istanza EC2 passano un ruolo IAM a un'istanza EC2. L'associa zione di un profilo dell'istanza alle istanze può facilitare la gestione delle autorizzazioni e del privilegio minimo.
5.1	iam-policy-no-statements-with-full-access	Assicurati che le azioni IAM siano limitate alle sole azioni necessarie. Concedere agli utenti più privilegi del necessario per completar e un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
5.1	iam-root-access-key-check	L'accesso ai sistemi e agli asset può essere controlla to controllando che l'utente root non disponga di chiavi di accesso associate al proprio ruolo AWS Identity and Access Management (IAM). Assicurati che le chiavi di accesso root vengano eliminate. Create e utilizzate invece sistemi basati sui ruoli Account AWS per contribuire a incorporare il principio della minima funzionalità.

ID controllo	AWS Regola di configurazione	Linea guida
5.1	iam-user-group-membership-check	AWS Identity and Access Management (IAM) può aiutarti a limitare i permessi e le autorizzazioni di accesso, assicurando che gli utenti siano membri di almeno un gruppo. Concedere agli utenti più privilegi del necessario per completare un'attività può violare il principio del privilegio minimo e della separazione dei compiti.
5.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) può aiutarti con i permessi e le autorizzazioni di accesso controllando le password e le chiavi di accesso IAM che non vengono utilizzate per un periodo di tempo specificato. Se rilevi credenziali inutilizzate, devi disabilitarle e/o rimuoverle, poiché ciò potrebbe violare il principio del privilegio minimo. Questa regola richiede di impostare un valore su maxCredentialUsageAge (Config Default: 90). Il valore effettivo deve essere conforme alle policy dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
5.4	secretsmanager-rotation-enabled-check	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto.
5.4	secretsmanager-scheduled-rotation-success-check	Questa regola garantisce che AWS i segreti di Secrets Manager siano ruotati correttamente in base alla pianificazione di rotazione. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione.

ID controllo	AWS Regola di configurazione	Linea guida
5.4	secretsmanager-secret-periodic-rotation	Questa regola garantisce che AWS i segreti di Secrets Manager abbiano la rotazione periodica abilitata. La rotazione dei segreti secondo una pianificazione regolare può abbreviare il periodo di attività di un segreto e ridurre potenzialmente l'impatto aziendale in caso di compromissione del segreto. Il valore predefinito è 90 giorni.
5.4	secretsmanager-using-cmk	Per proteggere i dati archiviati, assicurati che la crittografia con AWS Key Management Service (AWS KMS) sia abilitata per AWS i segreti di Secrets Manager. Data la possibile presenza di dati sensibili a riposo nei segreti di Secrets Manager, abilita la crittografia a riposo per proteggere tali dati.
6.4	ec2-instance-detailed-monitoring-enabled	Abilita questa regola per migliorare il monitoraggio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) sulla console Amazon EC2, che visualizza grafici di monitoraggio relativi all'istanza a intervalli di 1 minuto.

ID controllo	AWS Regola di configurazione	Linea guida
6.4	cloudwatch-log-group-encrypted	Per proteggere i dati sensibili archiviati, assicurati che la crittografia sia abilitata per i tuoi Amazon CloudWatch Log Groups.
6.4	cloud-trail-cloud-watch-logs-enabled	Usa Amazon CloudWatch per raccogliere e gestire centralmente l'attività degli eventi di registro. L'inclusione dei AWS CloudTrail dati fornisce dettagli sull'attività delle chiamate API all'interno del tuo Account AWS.
6.4	cloudtrail-enabled	AWS CloudTrail può contribuire a evitare il ripudio registrando le azioni della Console di AWS gestione e le chiamate API. È possibile identificare gli utenti e gli utenti Account AWS che hanno chiamato un AWS servizio, l'indirizzo IP di origine da cui sono state generate le chiamate e gli orari delle chiamate. I dettagli dei dati acquisiti sono visualizzati in AWS CloudTrail Record Contents.
6.4	cloud-trail-encryption-enabled	Poiché possono esistere dati sensibili e per proteggere i dati archiviati, assicurati che la crittografia sia abilitata per i tuoi AWS CloudTrail percorsi.

ID controllo	AWS Regola di configurazione	Linea guida
6.4	cloud-trail-log-file-validation-enabled	Utilizza la convalida dei file di AWS CloudTrail registro per verificare l'integrità dei CloudTrail registri. La convalida dei file di registro consente di determinare se un file di registro è stato modificato o eliminato o è rimasto invariato dopo la consegna. CloudTrail Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail
6.4	ec2-stopped-instance	Abilita questa regola per facilitare la configurazione di base delle istanze Amazon Elastic Compute Cloud (Amazon EC2) verificando se le istanze Amazon EC2 sono state interrotte per un numero di giorni superiore a quello consentito, secondo gli standard dell'organizzazione.

ID controllo	AWS Regola di configurazione	Linea guida
6.4	vpc-flow-logs-enabled	I log di flusso VPC forniscon o record dettagliati sul traffico IP da e verso le interfacce di rete nell'Amazon Virtual Private Cloud (Amazon VPC). Per impostazione predefinita il record del log di flusso include valori per i vari componenti del flusso IP, tra cui origine, destinazione e protocollo.
6.5A	guardduty-enabled-centralized	Amazon GuardDuty può aiutarti a monitorare e rilevare potenziali eventi di sicurezza informatica utilizzando feed di intelligence sulle minacce. Questi includono elenchi di IP dannosi e apprendim ento automatico per identific are attività impreviste, non autorizzate e dannose all'inter no del tuo AWS ambiente cloud.

ID controllo	AWS Regola di configurazione	Linea guida
6.5A	securityhub-enabled	AWS Security Hub aiuta a monitorare personale, connessioni, dispositivi e software non autorizzati. AWS Security Hub aggrega, organizza e dà priorità agli avvisi di sicurezza, o risultati , provenienti da più servizi. AWS Alcuni di questi servizi sono Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer e AWS Firewall Manager e soluzioni Partner. AWS

Modello

Il modello è disponibile su GitHub: Operational Best Practices for SWIFT CSP.

Best practice di sicurezza per Amazon Elastic Container Service (Amazon ECS)

Questo pacchetto di conformità contiene AWS Config regole basate su Amazon ECS. Per un elenco di tutte le regole gestite supportate da AWS Config, consulta Elenco delle AWS Config regole gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for Amazon ECS.

Best practice di sicurezza per Amazon Elastic File System (Amazon EFS)

Questo pacchetto di conformità contiene AWS Config regole basate su Amazon EFS. Per un elenco di tutte le regole gestite supportate da AWS Config, consulta Elenco delle regole AWS Config gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for Amazon EFS.

Best practice di sicurezza per Amazon Elastic Kubernetes Service (Amazon EKS)

Questo pacchetto di conformità contiene AWS Config regole basate su Amazon EKS. Per un elenco di tutte le regole gestite supportate da AWS Config, consulta Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for Amazon EKS.

Best practice di sicurezza per Amazon CloudFront

Questo pacchetto di conformità contiene AWS Config regole basate su Amazon. CloudFront Per un elenco di tutte le regole gestite supportate da AWS Config, consulta Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for Amazon CloudFront.

Best practice di sicurezza per Amazon OpenSearch Service

Questo pacchetto di conformità contiene AWS Config regole basate su Amazon OpenSearch Service. Per un elenco di tutte le regole gestite supportate da AWS Config, consulta Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for Amazon OpenSearch Service.

Best practice di sicurezza per Amazon Redshift

Questo pacchetto di conformità contiene AWS Config regole basate su Amazon Redshift. Per un elenco di tutte le regole gestite supportate da AWS Config, consulta Elenco delle AWS Config regole gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for Amazon Redshift.

Best practice di sicurezza per Amazon Relational Database Service (Amazon RDS)

Questo pacchetto di conformità contiene AWS Config regole basate su Amazon RDS. Per un elenco di tutte le regole gestite supportate da AWS Config, consulta Elenco delle AWS Config regole gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for Amazon RDS.

Best practice di sicurezza per AWS Auto Scaling

Questo pacchetto di conformità contiene AWS Config regole basate su. AWS Auto Scaling Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for AWS Auto Scaling.

Best practice di sicurezza per AWS CloudTrail

Questo pacchetto di conformità contiene AWS Config regole basate su. AWS CloudTrail Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for AWS CloudTrail.

Best practice di sicurezza per AWS CodeBuild

Questo pacchetto di conformità contiene AWS Config regole basate su. AWS CodeBuild Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for AWS CodeBuild.

Best practice di sicurezza per Amazon ECR

Questo pacchetto di conformità contiene AWS Config regole basate su Amazon Elastic Container Registry (Amazon ECR). Per un elenco di tutte le regole gestite supportate da AWS Config, consulta Elenco delle AWS Config regole gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for Amazon ECR.

Best practice di sicurezza per AWS Lambda

Questo pacchetto di conformità contiene AWS Config regole basate su. AWS Lambda Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for AWS Lambda.

Best practice di sicurezza per AWS Network Firewall

Questo pacchetto di conformità contiene AWS Config regole basate su. AWS Network Firewall Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for AWS Network Firewall.

Best practice di sicurezza per Amazon SageMaker

Questo pacchetto di conformità contiene AWS Config regole basate su Amazon. SageMaker Per un elenco di tutte le regole gestite supportate da AWS Config, consulta Elenco delle regole AWS Config gestite.

Consulta la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for Amazon SageMaker.

Best practice di sicurezza per AWS Secrets Manager

Questo pacchetto di conformità contiene AWS Config regole basate su. AWS Secrets Manager Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for AWS Secrets Manager.

Best practice di sicurezza per AWS WAF

Questo pacchetto di conformità contiene AWS Config regole basate su. AWS WAF Per un elenco di tutte le regole gestite supportate da AWS Config, vedi Elenco delle regole AWS Config gestite.

Vedi la `Parameters` sezione del modello seguente per i nomi e le descrizioni dei parametri richiesti.

Il modello è disponibile su GitHub: Security Best Practices for AWS WAF.

Modelli di esempio con azione di correzione

Migliori pratiche operative per Amazon DynamoDB con correzione

Il modello è disponibile su GitHub: Migliori pratiche operative per Amazon DynamoDB con correzione.

Best practice operative per Amazon S3 con correzione

Il modello è disponibile su GitHub: Best practice operative per Amazon S3 con correzione.

Per ulteriori informazioni sulla struttura del modello, vedere Template Anatomy nella Guida per l'utente. AWS CloudFormation

Pacchetti di conformità personalizzati

Un pacchetto di conformità personalizzato è una raccolta unica di AWS Config regole e azioni correttive che è possibile implementare insieme in un account e in una AWS regione o all'interno di un'organizzazione in. AWS Organizations

Per creare un pacchetto di conformità personalizzato, segui la procedura indicata nella seguente sezione Personalizzazione del modello per creare un file YAML che contenga l'elenco delle regole gestite da AWS Config o delle regole AWS Config personalizzate con cui desideri lavorare.

Terminologia

AWS Config Le Managed Rules sono regole predefinite di proprietà di. AWS Config

AWS Config Le regole personalizzate sono regole create da zero.

Esistono due modi per creare regole AWS Config personalizzate: con le funzioni Lambda (AWS Lambda Developer Guide) e con Guard (Guard GitHub Repository), un linguaggio. policy-as-code AWS Config le regole personalizzate create con AWS Lambda sono chiamate Regole Lambda AWS Config personalizzate e le regole AWS Config personalizzate create con Guard sono chiamate Regole di policy AWS Config personalizzate.

Personalizzazione del modello

Creazione del file YAML

Per creare un file YAML, apri un editor di testo e salva il file come .yaml.

> **Note**
>
> Il file contiene le sezioni Parametri e Risorse.

Parametri

La `Parameters` sezione del file YAML contiene i parametri delle regole per il set di AWS Config regole che aggiungerai più avanti nella sezione. `Resources` Crea la sezione `Parameters` copiando e incollando il seguente blocco di codice nel file YAML, personalizzandolo secondo necessità e ripetendo l'operazione per ogni parametro della regola.

```
Parameters:
    NameOfRuleParamNameOfRuleParameter:
        Default: Parameter value
        Type: Type
    ...
```

Per esempio:

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
```

> **Note**
>
> Quando selezioni le AWS Config Regole per creare il tuo pacchetto di conformità personalizzato, verifica che all'interno del tuo account siano disponibili le risorse che verranno valutate in base alle Regole. AWS Config

1. La prima riga nella sezione dei parametri che segue `Parameters:` è una stringa concatenata di + Param +. *`NameOfRuleNameOfRuleParameter`*
   a. Sostituisci *`NameOfRule`* con un nome coerente creato per la regola. Ad esempio, potrebbe essere IamPasswordPolicyper la regola. iam-password-policy
   b. Tipo `Param`.
   c. Quindi, sostituisci *`NameOfRuleParameter`* con il nome del parametro della regola specifica. Per AWS Config Managed Rules, il nome del parametro della regola si trova nell'Elenco delle regole AWS Config gestite (ad esempio, MinimumPasswordLengthè il nome di un parametro di regola per la iam-password-policyregola). Per le regole AWS Config personalizzate, il nome del parametro della regola è il nome scelto al momento della creazione della regola.
2. Se utilizzi una regola AWS Config gestita, trova la AWS Config regola appropriata nell'elenco delle regole gestite in modo da conoscere i valori accettati per `Default` e `Type` per la tua regola specifica. Per le regole AWS Config personalizzate, utilizza i valori selezionati durante la creazione della regola.

   > **Note**
   >
   > Per ogni parametro, `Type` deve essere specificato. `Type`può essere uno tra «String», «int», «double», «CSV», «boolean» e "». StringMap

Risorse

La sezione `Resources` elenca le regole che vengono aggiunte al pacchetto di conformità personalizzato. Aggiungi il seguente blocco `Resources` direttamente sotto la sezione `Parameters`, personalizzandolo secondo necessità e ripetendo l'operazione per ogni regola. Per ulteriori informazioni sulle specifiche, vedere. AWS::Config::ConfigRule

```
Resources:
     NameOfRule:
        Properties:
            ConfigRuleName: ActualConfigRuleName
            InputParameters:
                NameOfRuleParameter: NameOfRuleParamNameOfRuleParameter
            Source:
                Owner: Owner
                SourceIdentifier: SOURCE_IDENTIFIER
        Type: AWS::Config::ConfigRule
     ...
```

Per esempio:

```
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
```

> **Note**
>
> Quando selezioni le AWS Config regole per creare il tuo pacchetto di conformità personalizzato, verifica di disporre delle risorse che verranno valutate per le AWS Config regole previste all'interno del tuo account. Per ulteriori informazioni, consulta Tipi di risorsa supportati.

1. Sostituisci *`NameOfRule`* con lo stesso nome creato nella sezione `Parameters`.

2. Per AWS Config Managed Rules, *ActualConfigRuleName* sostituiscilo con il titolo della pagina delle regole appropriata nell'Elenco delle regole gestite. AWS Config Per le regole AWS Config personalizzate, usa il nome della regola di Config che hai scelto al momento della creazione della regola.
3. Sostituisci *NameOfRuleParameter* con lo stesso nome utilizzato nella sezione `Parameters`. Dopo i due punti, copia e incolla la stessa stringa concatenata di *NameOfRule*+ Param + *NameOfRuleParameter*che hai creato nella sezione. `Parameters`
4. Modifica *Owner* sul valore appropriato.

> **Note**
>
> AWS Config Regole gestite
> Per AWS Config Managed Rules, il valore per `Owner` sarà`AWS`.
> AWS Config Regole personalizzate
> Per le regole AWS Config personalizzate create con Guard, il valore per `Owner` sarà`CUSTOM_POLICY`. Per le regole AWS Config personalizzate create con Lambda, il valore per `Owner` sarà. `CUSTOM_LAMBDA`

5. Modifica *SOURCE_IDENTIFIER* sul valore appropriato.

> **Note**
>
> AWS Config Regole gestite
> Per le regole AWS Config gestite, copia l'identificatore seguendo il collegamento dalla regola selezionata dall'elenco delle regole AWS Config gestite (ad esempio, l'identificatore di origine della access-keys-rotatedregola è ACCESS_KEYS_ROTATED).
> AWS Config Regole personalizzate
> Per le regole AWS Config personalizzate create con Lambda, `SourceIdentifier` è l'Amazon Resource Name (ARN) della AWS Lambda funzione della regola, ad esempio. `arn:aws:lambda:us-east-2:123456789012:function:`*ActualConfigRuleName* Per le regole AWS Config personalizzate create con Guard, questo campo non è necessario.

Nel complesso, il pacchetto di conformità personalizzato compilato dovrebbe iniziare ad assomigliare al seguente, che è un esempio di utilizzo delle seguenti AWS Config Managed Rules: iam-password-policy, access-keys-rotatede -check. iam-user-unused-credentials

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
    AccessKeysRotatedParamMaxAccessKeyAge:
        Default: '90'
        Type: String
    IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge:
        Default: '45'
        Type: String
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
    AccessKeysRotated:
        Properties:
            ConfigRuleName: access-keys-rotated
            InputParameters:
                maxAccessKeyAge: AccessKeysRotatedParamMaxAccessKeyAge
            Source:
                Owner: AWS
                SourceIdentifier: ACCESS_KEYS_ROTATED
        Type: AWS::Config::ConfigRule
    IamUserUnusedCredentialsCheck:
        Properties:
            ConfigRuleName: iam-user-unused-credentials-check
            InputParameters:
                maxCredentialUsageAge:
 IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge
            Source:
                Owner: AWS
                SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
        Type: AWS::Config::ConfigRule
```

Implementazione del pacchetto di conformità personalizzato

Per distribuire un pacchetto di conformità personalizzato, consulta Distribuzione di un Conformance Pack utilizzando la AWS Config console e la distribuzione di un Conformance Pack utilizzando l'interfaccia a riga di comando. AWS Config

Visualizzazione dei dati di conformità nel pannello di controllo dei pacchetti di conformità

Nella pagina principale dei Pacchetti di conformità sono mostrati tutti i pacchetti di conformità attualmente presenti in Account AWS. La pagina contiene anche il nome, lo stato di implementazione e il punteggio di conformità di ogni pacchetto di conformità. Il punteggio di conformità è la percentuale del numero di combinazioni regola-risorsa conformi in un pacchetto di conformità rispetto al numero totale di combinazioni regola-risorsa possibili nel pacchetto di conformità.

Puoi utilizzare questo pannello di controllo per comprendere il livello di conformità dei pacchetti di conformità e utilizzare il punteggio di conformità per tenere traccia dell'avanzamento delle correzioni, eseguire confronti tra diversi set di requisiti e vedere l'impatto di una modifica o un'implementazione specifica su un pacchetto di conformità.

Esplorazione della pagina principale dei pacchetti di conformità

1. Accedi alla AWS Management Console e aprire la console di AWS Config all'indirizzo https://console.aws.amazon.com/config/.
2. Vai alla pagina Pacchetti di conformità. Esamina i pacchetti di conformità e i relativi punteggi di conformità. È anche possibile fare quanto segue:
   - Per aggiungere e configurare un nuovo pacchetto di conformità, scegli Distribuisci pacchetto di conformità.
   - Per eliminare un pacchetto di conformità e i relativi dati, modificare le impostazioni di configurazione o visualizzare dettagli aggiuntivi, come la posizione di consegna o i parametri, scegli un pacchetto di conformità e Azioni.

> **Note**
>
> Non puoi modificare un pacchetto di conformità implementato. Puoi modificare le altre selezioni in qualsiasi momento selezionando il nome del pacchetto di conformità e Modifica nel menu a discesa Azioni.

- Per visualizzare la cronologia delle modifiche allo stato di conformità, scegli un pacchetto di conformità e Timeline del pacchetto di conformità. Per ulteriori informazioni, consulta Visualizzazione della timeline della cronologia di conformità dei pacchetti di conformità.
- Per visualizzare lo stato di implementazione, il punteggio di conformità, la relativa timeline e le regole di un pacchetto di conformità in una vista dettagliata, scegli un pacchetto di conformità e Visualizza.

Ulteriori informazioni

Prerequisiti del pacchetto di conformità

Modelli di esempio di pacchetto di conformità

Implementazione di un pacchetto di conformità

Restrizioni dei servizi AWS

Visualizzazione della timeline della cronologia di conformità dei pacchetti di conformità

AWS Config supporta l'archiviazione delle modifiche dello stato di conformità nei pacchetti di conformità. Ciò consente di visualizzare la cronologia delle modifiche allo stato di conformità. Queste modifiche allo stato di conformità vengono presentate come una timeline. La timeline acquisisce le modifiche come `ConfigurationItems` in un intervallo di tempo. È inoltre possibile utilizzare questa funzionalità per trovare regole specifiche all'interno di un pacchetto di conformità che non sono conformi.

Puoi scegliere di registrare o meno tutti i tipi di risorse in AWS Config. Se si è scelto di registrare tutti i tipi di risorse, inizia AWS Config automaticamente a registrare la cronologia di conformità del Conformance Pack valutata da Rules. AWS Config Per impostazione predefinita, AWS Config registra le modifiche alla configurazione per tutte le risorse supportate. Puoi inoltre

selezionare solo il tipo di risorsa relativo alla cronologia di conformità del pacchetto di conformità specifico: `AWS::Config::ConformancePackCompliance`. La registrazione del tipo di risorsa `AWS::Config::ConformancePackCompliance` è disponibile senza costi aggiuntivi. Per ulteriori informazioni, vedere Selezione dei AWS Config record di risorse.

Un pacchetto di conformità è conforme se tutte le regole al suo interno sono conformi. Non è conforme se una qualsiasi delle regole non lo è. Lo stato di conformità di un pacchetto di conformità è INSUFFICIENT_DATA solo se tutte le regole al suo interno non possono essere valutate a causa di dati insufficienti. Se alcune delle regole di un pacchetto di conformità sono conformi, ma lo stato di conformità di altre regole nello stesso pacchetto di conformità è INSUFFICIENT_DATA, il pacchetto di conformità risulta conforme. La conformità di un pacchetto di conformità non viene valutata tutto in una volta. La valutazione di alcune regole può richiedere più tempo rispetto ad altre. La conformità viene valutata per gruppi di regole e prosegue per fasi finché non vengono valutate tutte le regole all'interno del pacchetto di conformità.

Argomenti

- Visualizzazione della timeline di conformità
- Query sulla cronologia di conformità

Visualizzazione della timeline di conformità

Accedi alla timeline di conformità selezionando un pacchetto di conformità specifico dalla pagina principale Pacchetto di conformità

1. Vai alla pagina Pacchetto di conformità.
2. Nella pagina principale Pacchetto di conformità, scegli un pacchetto di conformità specifico, quindi scegli Timeline del pacchetto di conformità.

> **Note**
>
> In alternativa, puoi utilizzare la timeline di conformità dalla pagina dei dettagli del pacchetto di conformità. Scegli un pacchetto di conformità, quindi Visualizza dettagli nel menu a discesa Operazioni. In questa pagina, scegli Timeline del pacchetto di conformità.

La timeline mostra la cronologia delle modifiche allo stato di conformità di un pacchetto di conformità. Puoi eseguire le operazioni indicate di seguito:

1. Espandi una modifica di conformità per visualizzare lo stato di line-by-line conformità di ogni regola all'interno di un pacchetto di conformità.
2. Dalla vista estesa, scegli una regola specifica per visualizzare la relativa pagina dei dettagli.

Query sulla cronologia di conformità

Esegui una query sulla cronologia della conformità get-resource-config-history utilizzando il tipo di risorsa. `AWS::Config::ConformancePackCompliance`

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ConformancePackCompliance --resource-id conformance-pack-ID
```

Verrà visualizzato un output simile al seguente:

```
{
    "configurationItems": [
        {
            "version": "1.3",
            "accountId": "Account ID",
            "configurationItemCaptureTime": 1614641951.442,
            "configurationItemStatus": "OK",
            "configurationStateId": "1614641951442",
            "configurationItemMD5Hash": "",
            "arn": "arn:aws:config:us-east-1:Account ID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
```

```
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        },
        {
            "version": "1.3",
            "accountId": "768311917693",
            "configurationItemCaptureTime": 1605551029.515,
            "configurationItemStatus": "ResourceDiscovered",
            "configurationStateId": "1605551029515",
            "configurationItemMD5Hash": "",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        }
    ]
}
```

Per ulteriori informazioni, consulta Supported Resource Types (AWS Config) e GetResourceConfigHistorynel riferimento all'API.

Distribuzione di un pacchetto di conformità utilizzando la console AWS Config

Nella pagina Conformance packs (Pacchetti di conformità) è possibile distribuire un pacchetto di conformità per un account in una regione. È inoltre possibile modificare ed eliminare il pacchetto di conformità distribuito.

Implementa un Conformance Pack utilizzando modelli

È possibile implementare un pacchetto di conformità utilizzando modelli di AWS Config esempio o un modello personalizzato. Per istruzioni su come creare pacchetti di conformità personalizzati, vedere Custom Conformance Pack.

1. Accedi alla AWS Management Console e aprire la console di AWS Config all'indirizzo https://console.aws.amazon.com/config/.
2. Passare alla pagina Conformance packs (Pacchetti di conformità) e scegliere Deploy conformance pack (Distribuisci pacchetto di conformità).
3. Nella pagina Specify template (Specifica modello) scegliere un modello di esempio o utilizzare un modello esistente. Per ulteriori informazioni, vedi Esempio di template.

   - Se scegli Usa modello di esempio, seleziona un modello di esempio dall'elenco a discesa dei modelli di esempio.

     Per informazioni sui contenuti di ciascun modello, consultare Modelli di esempio di pacchetto di conformità.
   - Se si seleziona Template is ready (Il modello è pronto), specificare l'origine del modello. Si tratta di un URI Amazon S3, di un AWS Systems Manager documento (documento SSM) o di un modello da caricare.

     Se il modello è superiore a 50 KB, caricarlo nel bucket S3 e selezionare il percorso del bucket S3. Ad esempio: s3://*bucketname/prefix*.

     > **Important**
     >
     > Choose Template è pronto se hai creato il file YAML del tuo pacchetto di conformità da zero in base a Custom Conformance Pack.

4. Seleziona Successivo.

5. Nella pagina Specify conformance pack details (Specifica i dettagli del pacchetto di conformità) digitare il nome del pacchetto di conformità.

   Il nome del pacchetto di conformità deve essere un nome univoco con una lunghezza massima di 256 caratteri alfanumerici. Il nome può contenere trattini ma non può contenere spazi.
6. Facoltativo: aggiungere un parametro.

   I parametri sono definiti nel modello e consentono di gestire e organizzare le risorse.
7. Seleziona Successivo.
8. Nella pagina Review and deploy (Rivedi e distribuisci), esaminare tutte le informazioni.

   È possibile modificare i dettagli del modello e i dettagli del pacchetto di conformità scegliendo Edit (Modifica).
9. Scegliere Deploy conformance pack (Distribuisci pacchetto di conformità).

   AWS Config visualizza il pacchetto di conformità nella pagina del pacchetto di conformità con lo stato appropriato.

   Se la distribuzione del pacchetto di conformità non riesce, controllare le autorizzazioni, verificare di aver eseguito i passaggi prerequisiti e riprovare. Oppure puoi contattareAWS Support.

Per distribuire un pacchetto di conformità utilizzando un modello di esempio con correzioni, consulta Prerequisiti per l'utilizzo di un pacchetto di conformità con correzione e quindi la procedura precedente.

Per distribuire un pacchetto di conformità con una o più regole AWS Config, vedere Prerequisiti per l'utilizzo di un Conformance Pack con una o più regole AWS Config.

Modificare un pacchetto di conformità

1. Per modificare un pacchetto di conformità, selezionare il pacchetto di conformità dalla tabella.
2. Scegliere Actions (Operazioni), quindi scegliere Edit (Modifica).
3. Nella pagina Edit conformance pack (Modifica pacchetto di conformità) è possibile modificare i dettagli del modello, il modello di esempio, il pacchetto di conformità e la sezione dei parametri.

   Non è possibile modificare il nome del pacchetto di conformità.
4. Sceglie Save changes (Salva modifiche).

Il pacchetto di conformità viene visualizzato con le regole AWS Config.

Eliminare un pacchetto di conformità

1. Per eliminare un pacchetto di conformità, selezionare il pacchetto di conformità dalla tabella.
2. Scegliere Actions (Operazioni), quindi selezionare Delete (Elimina VPC).
3. Nella finestra di dialogo *`Delete conformance pack (Elimina pacchetto di conformità)`* confermare se si desidera eliminare definitivamente questo pacchetto di conformità.

   > **Important**
   >
   > Non è possibile annullare questa operazione. Quando si elimina un pacchetto di conformità, si eliminano tutte le regole e le operazioni di correzione AWS Config nel pacchetto di conformità.

4. Immettere Delete (Elimina) e scegliere Delete (Elimina).

   Nella pagina Conformance packs (Pacchetti di conformità) lo stato della distribuzione viene visualizzato come Eliminazione fino al completamento dell'eliminazione del pacchetto di conformità.

Distribuzione di un pacchetto di conformità utilizzando l' AWS Command Line Interface

È possibile distribuire, visualizzare, aggiornare, visualizzare lo stato di conformità ed eliminare un pacchetto di AWS Config conformità utilizzando (). AWS Command Line Interface AWS CLI

AWS CLI È uno strumento unificato per gestire i tuoi servizi. AWS Con un solo strumento da scaricare e configurare, puoi controllare più AWS servizi dalla riga di comando e utilizzare script per automatizzarli. Per ulteriori informazioni sugli strumenti AWS CLI e per istruzioni sull'installazione degli AWS CLI strumenti, vedere quanto segue nella Guida per l'AWS Command Line Interface utente.

- AWS Command Line Interface Guida per l'utente
- Come configurare la AWS Command Line Interface

Se necessario, digitare `aws configure` per configurare l'utilizzo AWS CLI di una AWS regione in cui sono disponibili pacchetti di conformità.

Argomenti

- Distribuire un pacchetto di conformità
- Visualizzare un pacchetto di conformità
- Visualizzare lo stato del pacchetto di conformità
- Visualizzare lo stato di conformità del pacchetto di conformità
- Ottenere i dettagli di conformità per un pacchetto di conformità specifico
- Eliminare un pacchetto di conformità

Distribuire un pacchetto di conformità

1. Apri un prompt dei comandi o una finestra del terminale.
2. Digita uno dei comandi seguenti per implementare un pacchetto di conformità denominato **`MyConformancePack`**. L'origine del modello è un URI Amazon S3, un modello che carichi o un AWS Systems Manager documento (documento SSM).

   URI Amazon S3

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-s3-uri "s3://AmazonS3BucketName/templateName.yaml"
   --delivery-s3-bucket AmazonS3BucketName
   ```

   Modello YAML dalla directory locale

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-body template body
   ```

   AWS Systems Manager Documento (documento Systems Manager)

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-ssm-document-details
    DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
   ```

```
--delivery-s3-bucket AmazonS3BucketName
```

3. Premere Invio per eseguire il comando.

   Verrà visualizzato un output simile al seguente.

```
{
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID"
}
```

> **Note**
>
> Per ulteriori informazioni sulla creazione di un modello YAML per un pacchetto di conformità, consulta Pacchetto di conformità personalizzato.

Visualizzare un pacchetto di conformità

1. Inserire il seguente comando.

```
aws configservice describe-conformance-packs
```

   O

```
aws configservice describe-conformance-packs --conformance-pack-
name="MyConformancePack1"
```

2. Verrà visualizzato un output simile al seguente.

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID",
    "conformancePackInputParameters": [],
    "lastUpdateRequestedTime": "Thu Jul 18 16:07:05 PDT 2019"
}
```

Visualizzare lo stato del pacchetto di conformità

1. Inserire il seguente comando.

```
aws configservice describe-conformance-pack-status --conformance-pack-
name="MyConformancePack1"
```

2. Verrà visualizzato un output simile al seguente.

```
{
    "stackArn": "arn:aws:cloudformation:us-west-2:AccountID:stack/
awsconfigconforms-MyConformancePack1-conformance-pack-ID/d4301fe0-
a9b1-11e9-994d-025f28dd83ba",
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "lastUpdateCompletedTime": "Thu Jul 18 16:15:17 PDT 2019",
    "conformancePackState": "CREATE_COMPLETE",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID",
    "lastUpdateRequestedTime": "Thu Jul 18 16:14:35 PDT 2019"
}
```

Visualizzare lo stato di conformità del pacchetto di conformità

1. Inserire il seguente comando.

```
aws configservice describe-conformance-pack-compliance --conformance-pack-
name="MyConformancePack1"
```

2. Verrà visualizzato un output simile al seguente.

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackRuleComplianceList": [
        {
            "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
            "complianceType": "COMPLIANT"
```

```
        }
    ]
}
```

Ottenere i dettagli di conformità per un pacchetto di conformità specifico

1. Inserire il seguente comando.

```
aws configservice get-conformance-pack-compliance-details --conformance-pack-
name="MyConformancePack1"
```

2. Verrà visualizzato un output simile al seguente.

```
{
    "conformancePackRuleEvaluationResults": [
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Tue Jul 16 23:07:35 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName1-conformance-
pack-ID",
                    "resourceType": "AWS::::Account"
                }
            },
            "configRuleInvokedTime": "Tue Jul 16 23:07:50 PDT 2019",
            "resultRecordedTime": "Tue Jul 16 23:07:51 PDT 2019",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Thu Jun 27 15:16:36 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName2-conformance-
pack-ID",
                    "resourceType": "AWS::EC2::SecurityGroup"
                }
            },
           "configRuleInvokedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "resultRecordedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "complianceType": "COMPLIANT"
```

```
        }
    ],
    "conformancePackName": "MyConformancePack1"
}
}
```

Eliminare un pacchetto di conformità

Inserire il seguente comando.

```
aws configservice delete-conformance-pack --conformance-pack-name MyConformancePack1
```

In caso di esito positivo, il comando viene eseguito senza ulteriore output.

> **Important**
>
> Non è possibile annullare questa operazione. Quando si elimina un pacchetto di conformità, si eliminano tutte le AWS Config regole e le azioni correttive in esso contenute.

Gestione dei pacchetti di conformità (API)

Utilizza le seguenti azioni AWS Config API per gestire i pacchetti di conformità:

- DeleteConformanceImballa, elimina il pacchetto di conformità specificato e tutte le AWS Config regole e tutti i risultati di valutazione all'interno di tale pacchetto.
- DescribeConformancePackCompliance, restituisce le informazioni sulla conformità per ogni regola del pacchetto di conformità.
- DescribeConformancePacchetti, restituisce un elenco di uno o più pacchetti di conformità.
- DescribeConformancePackStatus, fornisce lo stato di implementazione di uno o più pacchetti di conformità.
- GetConformancePackComplianceDettagli, restituisce i dettagli di conformità di un pacchetto di conformità per tutte le AWS risorse monitorate dal pacchetto di conformità.
- GetConformancePackComplianceRiepilogo, restituisce le informazioni sulla conformità per il pacchetto di conformità in base ai risultati cumulativi di conformità di tutte le regole di tale pacchetto di conformità.

- ListConformancePackCompliancePunteggi, restituisce un elenco dei punteggi di conformità del pacchetto di conformità.
- PutConformanceComprimi, crea o aggiorna un pacchetto di conformità.

Gestione dei pacchetti di conformità in tutti gli account dell'organizzazione

AWS Config Utilizzatelo per gestire i pacchetti di conformità in tutta Account AWS l'organizzazione. Puoi eseguire le operazioni indicate di seguito:

- Distribuire, aggiornare ed eliminare centralmente i pacchetti di conformità tra gli account membri in un'organizzazione in AWS Organizations.
- Implementa un insieme comune di AWS Config regole e azioni correttive in tutti gli account e specifica gli account in cui non devono essere create AWS Config regole e azioni correttive.
- Utilizza l'account di gestione AWS Organizations per applicare la governance assicurandoti che AWS Config le regole e le azioni correttive sottostanti non siano modificabili dagli account dei membri dell'organizzazione.

Considerazioni

Per le implementazioni in diverse regioni

La chiamata API per distribuire regole e pacchetti di conformità tra gli account è specifica della regione. AWS A livello di organizzazione, è necessario modificare il contesto della chiamata API su un'altra regione se desideri implementare le regole in altre regioni. Ad esempio, per implementare una regola negli Stati Uniti orientali (Virginia settentrionale), modifica la regione in Stati Uniti orientali (Virginia settentrionale) e quindi chiama `PutOrganizationConfigRule`.

Per gli account all'interno di un'organizzazione

Se un nuovo account entra a far parte di un'organizzazione, la regola o il pacchetto di conformità vengono implementati in quell'account. Quando un account lascia un'organizzazione, la regola o il pacchetto di conformità vengono rimossi.

Se implementi una regola o un pacchetto di conformità organizzativi in un account amministratore dell'organizzazione e quindi stabilisci un amministratore delegato e implementi una regola o un pacchetto di conformità organizzativi nell'account amministratore delegato, non potrai visualizzare

la regola o il pacchetto di conformità organizzativi nell'account amministratore dell'organizzazione dall'account amministratore delegato o visualizzare la regola o il pacchetto di conformità organizzativi nell'account amministratore delegato dall'account amministratore dell'organizzazione. Le DescribeOrganizationConformancePacksAPI DescribeOrganizationConfigRulese possono solo visualizzare e interagire con le risorse relative all'organizzazione che sono state distribuite dall'account che chiama tali API.

Meccanismo di tentativi per i nuovi account aggiunti a un'organizzazione

Se non è disponibile un registratore, l'implementazione delle regole e dei pacchetti di conformità organizzativi esistenti viene ritentata solo per 7 ore dopo l'aggiunta di un account all'organizzazione. È necessario creare un registratore, se non ne esiste uno, entro 7 ore dall'aggiunta di un account all'organizzazione.

Account di gestione dell'organizzazione, amministratori delegati e ruoli collegati ai servizi

Se utilizzi un account di gestione dell'organizzazione e intendi utilizzare un amministratore delegato per la distribuzione organizzativa, tieni presente che questo AWS Config non creerà automaticamente il ruolo collegato al servizio (SLR). È necessario creare manualmente il ruolo collegato al servizio (SLR) separatamente utilizzando IAM.

Se non disponi di una reflex per il tuo account di gestione, non sarai in grado di distribuire risorse su quell'account da un account amministratore delegato. Sarete comunque in grado di distribuire pacchetti di conformità agli account dei membri dagli account di gestione e dagli account di amministratore delegato. Per ulteriori informazioni, consulta Using service-linked roles nella Guida per l'AWS Identity and Access Management utente (IAM).

Implementazione

To deploy with the AWS Management Console

Per distribuire un pacchetto di conformità in un'organizzazione dalla console, usa. AWS AWS Systems ManagerPer ulteriori informazioni, consulta Distribuire i AWS Config conformance pack nella Guida per l'utente.AWS Systems Manager

To deploy with the AWS API

Per informazioni su come eseguire l'integrazione AWS Config con AWS Organizations, consulta AWS Config e AWS Organizations nella Guida per l'AWS Organizations utente. Assicurati che AWS Config la registrazione sia attiva prima di utilizzare le seguenti API per gestire le regole del Conformance Pack in tutta l' Account AWS organizzazione:

- DeleteOrganizationConformancePack, elimina il pacchetto di conformità dell'organizzazione specificato e tutte le regole di configurazione e le azioni correttive da tutti gli account membri dell'organizzazione.
- DescribeOrganizationConformancePacks, restituisce un elenco di pacchetti di conformità dell'organizzazione.
- DescribeOrganizationConformancePackStatuses, fornisce lo stato di implementazione del pacchetto di conformità dell'organizzazione per un'organizzazione.
- GetOrganizationConformancePackDetailedStatus, restituisce lo stato dettagliato di ogni account membro all'interno di un'organizzazione per un determinato pacchetto di conformità dell'organizzazione.
- PutOrganizationConformancePack, distribuisce pacchetti di conformità tra gli account dei membri di un'organizzazione. AWS

Supporto nelle regioni

La distribuzione dei pacchetti di conformità tra gli account dei membri di un' AWS organizzazione è supportata nelle seguenti regioni.

Nome della regione	Regione	Endpoint	Protocollo
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Stati Uniti occidentali (California settentrionale)	us-west-1	config.us-west-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Asia Pacifico (Giacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pacifico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacifico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacifico (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacifico (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacifico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Canada (Centrale)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europa (Francoforte)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londra)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Parigi)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Sud America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Risoluzione dei problemi

Stato di errore per un pacchetto di conformità

Se viene visualizzato un errore che indica che il pacchetto di conformità non è riuscito durante la creazione, l'aggiornamento o l'eliminazione, è possibile verificare lo stato del pacchetto di conformità.

```
aws configservice describe-conformance-pack-status --conformance-pack-name
 MyConformancePack1
```

Verrà visualizzato un output simile al seguente.

```
"ConformancePackStatusDetails": [
    {
        "ConformancePackName": "ConformancePackName",
        "ConformancePackId": "ConformancePackId",
        "ConformancePackArn": "ConformancePackArn",
        "ConformancePackState": "CREATE_FAILED",
        "StackArn": "CloudFormation stackArn",
        "ConformancePackStatusReason": "Failure Reason",
        "LastUpdateRequestedTime": 1573865201.619,
        "LastUpdateCompletedTime": 1573864244.653
    }
]
```

Verificare la presenza ConformancePackStatusReasondi informazioni sull'errore.

Quando stackArn è presente nella risposta

Se il messaggio di errore non è chiaro o se il malfunzionamento è dovuto a un errore interno, passa alla console AWS CloudFormation e procedi come segue:

1. Cercare StackArn dall'output.
2. Scegli la scheda Eventi dello CloudFormation stack e verifica la presenza di eventi non riusciti.

   Il motivo dello stato indica il motivo per cui il pacchetto di conformità non è riuscito.

Quando stackArn non è presente nella risposta

Se si riceve un errore durante la creazione di un pacchetto di conformità ma lo StackArn non è presente nella risposta di stato, la possibile ragione è che la creazione dello stack non è riuscita, è stata ripristinata ed è stato eliminato lo stack. CloudFormation Vai alla CloudFormation console e cerca gli stack che si trovano in uno stato Eliminato. Lo stack non riuscito potrebbe essere disponibile lì. Lo CloudFormation stack contiene il nome del pacchetto di conformità. Se trovi lo stack fallito, scegli la scheda Eventi dello CloudFormation stack e verifica la presenza di eventi non riusciti.

Se nessuno di questi passaggi ha funzionato e se il motivo dell'errore è un errore interno del servizio, riprova a eseguire l'operazione o contatta il AWS Support Centro.

Regole diverse in un pacchetto di conformità

L'implementazione di un pacchetto di conformità implica la creazione di uno AWS CloudFormation stack sottostante in background per distribuire le regole nel modello del pacchetto di conformità. Queste regole sono regole collegate ai servizi e non possono essere aggiornate o eliminate al di fuori del conformance pack.

Se si apportano modifiche allo CloudFormation stack sottostante, si verifica una situazione in cui il Conformance Pack e le relative regole diventano ingestibili. Queste regole ingestibili sono regole sospese.

Vai alla deriva tra lo CloudFormation stack e il pacchetto di conformità

È possibile aggiornare i nomi delle regole in un modello di conformance pack direttamente dalla console. CloudFormation Se si aggiorna il modello direttamente dalla CloudFormation console, ciò non aggiorna il pacchetto di conformità distribuito.

Questa deriva crea una regola sospesa. Se si tenta di eliminare la regola dal pacchetto di conformità, viene visualizzato un errore simile al seguente:

```
"An AWS service owns ServiceLinkedConfigRule. You do not have permissions to
 take action on this rule. (Service: AmazonConfig; Status Code: 400; Error Code:
 AccessDeniedException; Request ID: my-request-ID; Proxy: null)".
```

Se si tenta di eliminare il conformance pack, non è possibile eliminare la regola pendente e viene visualizzato un errore simile al seguente:

```
"User: arn:aws:sts::111122223333:assumed-role/AWSServiceRoleForConfigConforms/
AwsConfigConformsWorkflow is not authorized to perform: config:DeleteConfigRule on
 resource: my-dangling-rule
```

Per risolvere questo problema, procedi nel seguente modo:

1. Eliminare lo stack. Per ulteriori informazioni, consulta Eliminazione di uno stack sulla AWS CloudFormation console nella Guida per l'CloudFormation utente.
2. Eliminare il pacchetto di conformità utilizzando la AWS Config console o l'API Pack. DeleteConformance Se si tratta di un pacchetto di conformità organizzativo e utilizzi l'account di gestione o amministratore delegato, utilizza l'API. DeleteOrganizationConformancePack
3. Contatta il AWS Support Centro con l'Amazon Resource Name (ARN) delle regole pendenti nel pacchetto di conformità per aiutarti a ripulire il tuo account.

Per evitare questo problema, ricorda queste best practice:

- Non apportare mai aggiornamenti diretti allo CloudFormation stack di un pacchetto di conformità.
- Non cercate mai di apportare modifiche che creino deviazioni tra il pacchetto di conformità e lo stack sottostante. CloudFormation
- Il ruolo collegato al servizio (SLR) per i conformance pack non può essere modificato. Assicurati che le risorse che stai aggiornando facciano parte della politica di autorizzazione per la SLR.

CloudFormation Stack eliminato per un pacchetto di conformità

A meno che non vi siano differenze tra lo CloudFormation stack e il conformance pack, non è mai consigliabile eliminare le regole in un conformance pack o nel relativo stack direttamente dalla console. CloudFormation CloudFormation

Per risolvere il problema, contatta il AWS Support Centro con l'Amazon Resource Name (ARN) delle regole pendenti nel pacchetto di conformità per aiutarti a ripulire il tuo account.

Per evitare questo problema, ricorda queste best practice:

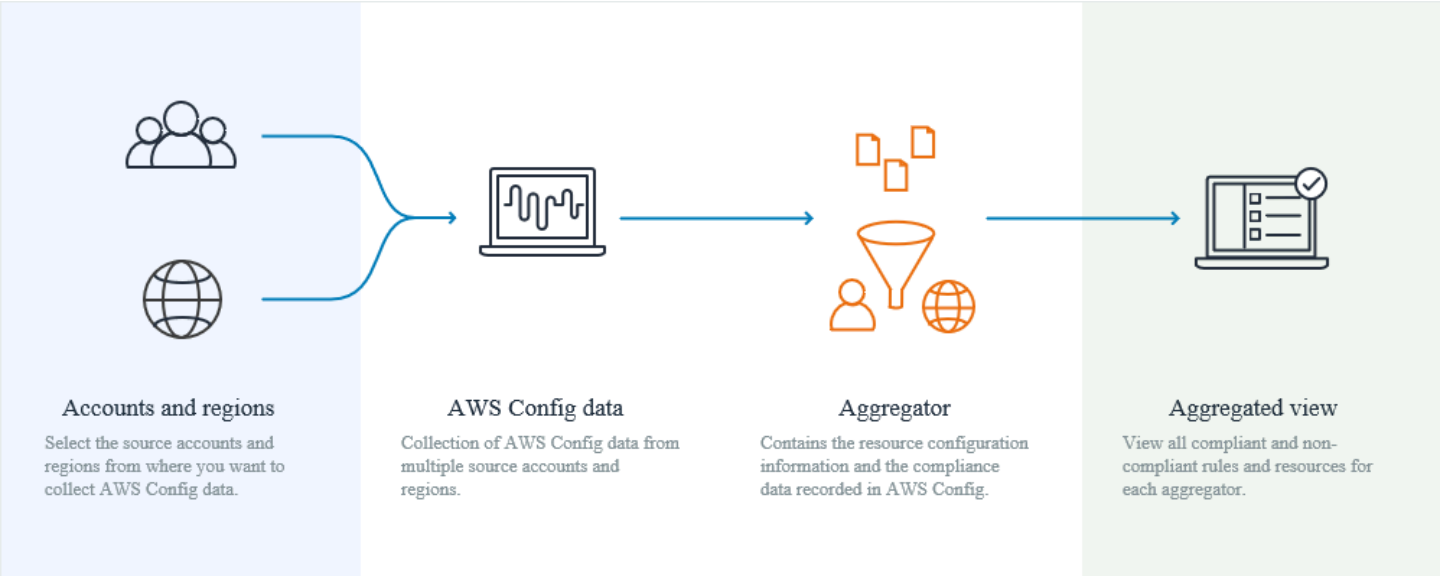
- Non eliminare mai lo CloudFormation stack sottostante di un pacchetto di conformità.
- Elimina i pacchetti di conformità utilizzando l'API Pack. DeleteConformance Se si tratta di un pacchetto di conformità organizzativa e utilizzi l'account di gestione o amministratore delegato, utilizza l'API. DeleteOrganizationConformancePack

Aggregazione di dati multi-regione multi-account

Un aggregatore è un tipo di AWS Config risorsa che raccoglie i dati di AWS Config configurazione e conformità dai seguenti elementi:

- Più account e più AWS regioni.
- Account singolo e più AWS regioni.
- Un'organizzazione AWS Organizations e tutti gli account di quell'organizzazione che sono stati AWS Config abilitati.

Utilizza un aggregatore di risorse per visualizzare i dati di configurazione della risorsa e di conformità registrati in AWS Config. Un aggregatore utilizza un bucket Amazon S3 per archiviare dati aggregati. Recupera periodicamente le istantanee di configurazione dagli account di origine e le archivia nel bucket S3 designato. L'immagine seguente mostra come un aggregatore raccoglie i AWS Config dati da più account e regioni.



Casi d'uso

- Monitoraggio della conformità: puoi aggregare i dati sulla conformità per valutare i livelli di conformità complessivi della tua organizzazione o di più account e regioni.
- Monitoraggio delle modifiche: puoi tenere traccia delle modifiche alle risorse nel tempo all'interno dell'organizzazione o tra account e regioni.

- Relazioni tra le risorse: puoi analizzare le dipendenze e le relazioni tra le risorse all'interno dell'organizzazione o tra account e regioni.

> **Note**
>
> Gli aggregatori forniscono una visualizzazione in sola lettura degli account e delle regioni di origine che l'aggregatore è autorizzato a visualizzare replicando i dati dagli account di origine nell'account di aggregazione. Gli aggregatori non forniscono un accesso mutante a un account o a una regione di origine. Ad esempio, ciò significa che non è possibile distribuire regole tramite un aggregatore o inviare file di istantanee a un account o a una regione di origine tramite un aggregatore.
> L'utilizzo degli aggregatori non comporta costi aggiuntivi.

Terminologia

Un account di origine è l'account Account AWS da cui si desidera aggregare i dati di configurazione e conformità AWS Config delle risorse. Un account di origine può essere un account singolo o un'organizzazione in AWS Organizations. Puoi fornire gli account di origine singolarmente o recuperarli tramite. AWS Organizations

Una regione di origine è la AWS regione da cui si desidera aggregare i dati di AWS Config configurazione e conformità.

Un account aggregatore è un account in cui si crea un aggregatore.

L'autorizzazione si riferisce alle autorizzazioni concesse a un account e a una regione di aggregazione per raccogliere i dati di AWS Config configurazione e conformità. L'autorizzazione non è obbligatoria se stai aggregando account di origine che fanno parte di AWS Organizations.

Come aggregare i dati

Per aggregare AWS Config i dati provenienti dagli account di origine e dalle regioni, inizia con:

1. Aggiungere un aggregatore per aggregare i dati di AWS Config configurazione e conformità provenienti da più account e regioni. Per ulteriori informazioni, consulta Impostazione di un aggregatore utilizzando la Console e Configurazione di un aggregatore utilizzando il AWS Command Line Interface.

2. Autorizzazione degli account aggregatori a raccogliere dati di AWS Config configurazione e conformità. Per ulteriori informazioni, consulta Autorizzazione degli account di aggregazione a raccogliere dati AWS Config di configurazione e conformità tramite la console e Autorizzazione degli account di aggregazione alla raccolta dei dati AWS Config di configurazione e conformità utilizzando AWS Command Line Interface.

> **Note**
>
> Esistono due tipi di aggregatori: aggregatore di account individuali e aggregatore di organizzazioni
> Per l'aggregatore di account individuali, è richiesta l'autorizzazione per tutte le Regioni degli account di origine incluse, comprese le Regioni degli account esterni o le Regioni degli account dei membri dell'organizzazione.
> Per l'aggregatore di organizzazioni, l'autorizzazione non è richiesta per le regioni degli account membri dell'organizzazione poiché l'autorizzazione è integrata con il servizio Organizations.

3. Monitoraggio dei dati di conformità per regole e account nella visualizzazione aggregata. Per ulteriori informazioni, consulta Visualizzazione dei dati di conformità e inventario nel pannello di controllo dell'aggregatore.

Supporto nelle regioni

Attualmente, l'aggregazione di dati multiregione con più account è supportata nelle seguenti regioni:

Nome della regione	Regione	Endpoint	Protocollo
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo	
Stati Uniti occidentali (California settentrionale)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
Asia Pacifico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Asia Pacific (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
Asia Pacifico (Giacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Asia Pacifico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacifico (Osaka-Locale)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacifico (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacifico (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacifico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Centrale)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Canada occidentale (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Europa (Francoforte)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londra)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milano)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Parigi)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spagna)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zurigo)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israele (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Medio Oriente (Bahrein)	me-south-1	config.me-south-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Medio Oriente (Emirati Arabi Uniti)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Sud America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Risoluzione dei problemi per l'aggregazione di dati da più account e regioni

AWS Config potrebbe non aggregare i dati dagli account di origine per uno dei seguenti motivi:

Se ciò accade	Esegui questa operazione
AWS Config non è abilitato nell'account di origine per gli account all'interno di un'organizzazione.	Abilita AWS Config nell'account di origine e autorizza l'account aggregatore a raccogliere dati.
L'autorizzazione non è concessa a un account dell'aggregatore.	Accedi all'account di origine e concedi l'autorizzazione all'account aggregatore per la raccolta dei dati. AWS Config
Potrebbe verificarsi un problema temporaneo che impedisce l'aggregazione dei dati.	L'aggregazione dei dati è soggetta a ritardi. Attendi alcuni minuti.

AWS Config potrebbe non aggregare i dati di un'organizzazione per uno dei seguenti motivi:

Se ciò accade	Esegui questa operazione
AWS Config non è in grado di accedere ai dettagli dell'organizzazione a causa di un ruolo IAM non valido.	Crea un ruolo IAM o seleziona un ruolo IAM valido dall'elenco dei ruoli IAM. **Note** Se il ruolo IAM non è valido per più di 24 ore, AWS Config elimina i dati dell'intera organizzazione.
AWS Config l'accesso al servizio è disabilitato nell'organizzazione.	È possibile abilitare l'integrazione tra AWS Config e AWS Organizations tramite l'`EnableAWSServiceAccess` API. Se scegli Aggiungi la mia organizzazione nella console, abilita AWS Config automaticamente l'integrazione tra AWS Config e AWS Organizations.
AWS Config non è in grado di accedere ai dettagli dell'organizzazion	Abilita tutte le funzionalità nella AWS Organizations console.

Se ciò accade	Esegui questa operazione
e perché tutte le funzionalità non sono abilitate nell'organizzazione.	
I cambiamenti organizzativi, come l'aggiunta e la rimozione di un account e l'abilitazione e la disabilitazione dell'accesso al servizio, non vengono aggiornati immediatamente nelle regioni Medio Oriente (Bahrein) e Asia Pacifico (Hong Kong).	I cambiamenti organizzativi sono soggetti a un ritardo di 2 ore. Attendi 2 ore per visualizzarli.

Visualizzazione dei dati di conformità e inventario nel pannello di controllo dell'aggregatore

La dashboard nella pagina Aggregatori mostra i dati di configurazione delle risorse AWS aggregate. Fornisce una panoramica delle regole, dei pacchetti di conformità e dei relativi stati di conformità.

La dashboard fornisce il numero totale di AWS risorse. I tipi e gli account di risorse vengono classificati in base al numero più elevato di risorse. Riporta inoltre il conteggio delle regole e dei pacchetti di conformità conformi e non conformi. Le regole non conformi sono classificate in base al numero più elevato di risorse non conformi. I pacchetti di conformità e gli account di origine non conformi sono classificati in base al numero più elevato di regole non conformi.

Dopo la configurazione AWS Config, inizia ad aggregare i dati dagli account di origine specificati in un aggregatore. Per visualizzare lo stato di conformità delle regole potrebbero essere necessari alcuni istanti.

Utilizzo del pannello di controllo dell'aggregatore

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Vai alla pagina Aggregatori. Puoi visualizzare:
   - Le regole e i relativi stati di conformità.
   - I pacchetti di conformità e i relativi stati di conformità.

- AWS Le tue risorse e i relativi dati di configurazione.

3. Scegli un aggregatore dal pannello di controllo. Filtra gli aggregatori in base al nome. Puoi visualizzare i widget seguenti:

   - Inventario risorse

     Visualizza i primi dieci tipi di risorse dall'aggregatore selezionato, in ordine decrescente, in base al numero di risorse. Scegli il numero totale di risorse per l'aggregatore selezionato, visualizzato tra parentesi dopo Inventario risorse, per accedere alla pagina Risorse aggregata, dove puoi visualizzare tutte le risorse di un aggregatore. In alternativa, scegli un tipo di risorsa nel widget per andare alla pagina Risorse aggregata, filtrata in base al tipo di risorsa specificato.

   - Account in base al numero di risorse

     Visualizza i primi cinque account dall'aggregatore selezionato, in ordine decrescente, in base al numero di risorse. Scegli un account nel widget per andare alla pagina Risorse, filtrata in base all'account specificato.

   - Regole non conformi

     Visualizza le prime cinque regole non conformi dall'aggregatore selezionato, in ordine decrescente, in base al numero di risorse non conformi. Scegli una regola nel widget per andare alla pagina dei dettagli corrispondente. Scegli Visualizza tutte le regole non conformi per andare alla pagina Regole aggregata, dove puoi visualizzare tutte le regole di un aggregatore.

   - Account in base alle regole non conformi

     Visualizza i primi cinque account dall'aggregatore selezionato, in ordine decrescente, in base al numero di regole non conformi. Scegli un account nel widget per andare alla pagina Regole aggregata, dove puoi visualizzare tutte le regole di un aggregatore filtrate in base all'account specificato.

   - Account per pacchetti di conformità non conformi

     Visualizza i primi cinque account dall'aggregatore selezionato, in ordine decrescente, in base al numero di pacchetti di conformità non conformi. Scegli un account nel widget per andare alla pagina Pacchetto di conformità aggregata, dove puoi visualizzare tutti i pacchetti di conformità di un aggregatore filtrati in base all'account specificato.

4. Nel riquadro di navigazione a sinistra, scegli una delle seguenti opzioni dal menu a discesa:

- Pannello di controllo della conformità

  Visualizza i pannelli di controllo della conformità automatizzati utilizzando i widget di riepilogo delle informazioni sulla conformità delle risorse all'interno dell'aggregatore. Puoi visualizzare dati come i primi dieci tipi di risorse in base alle risorse non conformi e i primi dieci pacchetti di conformità a livello di account in base alle regole non conformi. Per informazioni su questi grafici e diagrammi, consulta Pannelli di controllo della conformità.

- Pacchetti di conformità

  Visualizza tutti i pacchetti di conformità creati e collegati tra loro all' Account AWS interno del tuo aggregatore. Nella pagina Pacchetto di conformità viene visualizzata una tabella con il nome, la regione, l'ID dell'account e lo stato di conformità di ciascun pacchetto di conformità. Da questa pagina puoi scegliere un pacchetto di conformità e selezionare l'opzione Visualizza dettagli per ottenere ulteriori informazioni sulle relative regole e risorse e sullo stato di conformità.

- Regole

  Visualizza tutte le regole create e collegate ai diversi account AWS all'interno dell'aggregatore. Nella pagina Regole viene visualizzata una tabella con il nome, lo stato di conformità, la regione e l'account di ciascuna regola. Da questa pagina puoi scegliere una regola e selezionare l'opzione Visualizza dettagli per ottenere informazioni come l'aggregatore, la regione, l'ID dell'account e le risorse nell'ambito.

- Pannello di controllo dell'inventario

  Visualizza i pannelli di controllo dell'inventario automatizzati utilizzando i widget di riepilogo delle informazioni sui dati di configurazione delle risorse all'interno dell'aggregatore. Puoi visualizzare dati come i primi dieci tipi di risorse in base al numero di risorse e i primi dieci account in base al numero di risorse. Per informazioni su questi grafici e diagrammi, consulta Pannelli di controllo dell'inventario.

- Risorse

  Visualizza tutte le risorse registrate e collegate ai diversi account AWS all'interno dell'aggregatore. Dalla pagina Risorsa, scegli una risorsa e seleziona Visualizza dettagli per visualizzarne i dettagli, le regole ad essa associate e la configurazione corrente. Puoi anche visualizzare informazioni sulla risorsa, come l'aggregatore, la regione, l'ID account e il nome, il tipo e l'ID della risorsa.

- Autorizzazioni

  Visualizza e gestisci tutti gli account attualmente autorizzati o in attesa di autorizzazione. Dalla pagina Autorizzazioni, scegli Aggiungi autorizzazione per fornire l'accesso a un altro account. Scegli Elimina autorizzazione per revocare l'accesso da un ID dell'account.

> **Note**
>
> Risoluzione dei problemi
> Il messaggio Raccolta dei dati da tutti gli account e le regioni di origine incompleta viene visualizzato nella vista aggregata per i seguenti motivi:
>
> - Il trasferimento delle AWS Config regole non conformi e dei dati di configurazione delle risorse è in corso. AWS
> - AWS Config non riesco a trovare regole che corrispondano al filtro che hai applicato. Seleziona la regione o l'account appropriati e riprova.
>
> Potrebbe essere visualizzato questo messaggio nella vista aggregata: Raccolta dei dati dalla tua organizzazione incompleta. Puoi visualizzare i dati riportati di seguito solo per 24 ore. Questo messaggio viene visualizzato per le ragioni seguenti:
>
> - AWS Config non puoi accedere ai dettagli della tua organizzazione a causa di un ruolo IAM non valido. Se il ruolo IAM rimane non valido per più di 24 ore, AWS Config elimina i dati relativi all'intera organizzazione.
> - AWS Config l'accesso al servizio è disabilitato nell'organizzazione.

Pannello di controllo della conformità

Visualizza i pannelli di controllo della conformità automatizzati utilizzando widget di riepilogo delle informazioni sulla conformità delle risorse all'interno dell'aggregatore. Questo pannello di controllo mostra solo le regole con risultati di conformità.

> **Note**
>
> Limitazioni

Le informazioni contenute nel dashboard di conformità sono fornite dalla funzionalità Advanced Queries di AWS Config, che non supporta strutture annidate o la decompressione di array nidificati. Ciò significa che il dashboard di conformità mostra la conformità complessiva di una risorsa e non lo stato di conformità per ogni regola specifica che riporta su una risorsa.
Ad esempio, se si verifica l'elemento di configurazione (CI) per il tipo di risorsa`AWS::Config::ResourceCompliance`, il dashboard mostrerà i risultati di conformità per tutte le regole che generano report su quella risorsa. Se ci sono 10 regole che generano report sulla risorsa, 9 di esse sono CONFORMI e solo 1 è NON_COMPLIANT, la conformità complessiva di quella risorsa sarà NON_COMPLIANT.

Riepilogo della conformità per risorse

Visualizza un grafico a torta che confronta il numero di risorse conformi con quelle non conformi dell'aggregatore selezionato. Passa il mouse sul grafico per visualizzare il numero e la percentuale esatti di risorse conformi e non conformi.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato e dalle regioni in cui l'aggregatore selezionato è configurato per la raccolta dei dati.

I 10 principali tipi di risorse per risorse non conformi

Visualizza un grafico a barre orizzontale che confronta fino a 10 tipi di risorse dell'aggregatore selezionato in ordine decrescente in base al numero di risorse non conformi. Passa il mouse sul grafico per visualizzare il numero esatto di risorse non conformi per ogni tipo di risorsa.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato e dalle regioni in cui l'aggregatore selezionato è configurato per la raccolta dei dati.

I 10 account principali per risorse non conformi

I primi 10 account per risorse non conformi visualizza un grafico a barre orizzontali che confronta fino a 10 account dell'aggregatore selezionato in ordine decrescente in base al numero di risorse non conformi. Passa il mouse sul grafico per visualizzare il numero esatto di risorse non conformi per ogni account.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato e dalle regioni in cui l'aggregatore selezionato è configurato per la raccolta dei dati.

Le 10 principali regioni per risorse non conformi

Visualizza un grafico a barre orizzontale che confronta fino a 10 regioni in cui l'aggregatore selezionato raccoglie i dati in ordine decrescente in base al numero di risorse non conformi. Passa il mouse sul grafico per visualizzare il numero esatto di risorse non conformi per ogni regione.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato.

I 10 migliori pacchetti di conformità a livello di account in base alle regole non conformi

Visualizza un grafico a barre orizzontale che confronta fino a 10 pacchetti di conformità a livello di account dell'aggregatore selezionato in ordine decrescente in base al numero di regole non conformi. Passa il mouse sul grafico per visualizzare la percentuale di regole conformi e non conformi per ogni pacchetto di conformità a livello di account.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato e dalle regioni in cui l'aggregatore selezionato è configurato per la raccolta dei dati.

I 10 migliori pacchetti di conformità a livello di organizzazione in base alle regole non conformi

Visualizza un grafico a barre orizzontale che confronta fino a 10 pacchetti di conformità a livello organizzativo dell'aggregatore selezionato in ordine decrescente in base al numero di regole non conformi. Passa il mouse sul grafico per visualizzare la percentuale di regole conformi e non conformi in ogni pacchetto di conformità a livello organizzativo.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato e dalle regioni in cui l'aggregatore selezionato è configurato per la raccolta dei dati.

I 10 migliori account per regole non conformi tra i diversi pacchetti di conformità

I primi 10 account per regole non conformi tra i diversi pacchetti di conformità mostrano un grafico a barre orizzontali che confronta fino a 10 account dell'aggregatore selezionato in ordine decrescente in base al numero di regole non conformi in tutti i pacchetti di conformità. Passa il mouse sul grafico per visualizzare il numero esatto di regole non conformi in ogni account.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato e dalle regioni in cui l'aggregatore selezionato è configurato per la raccolta dei dati.

Pannello di controllo dell'inventario

Visualizza i pannelli di controllo dell'inventario automatizzati utilizzando i widget di riepilogo delle informazioni sui dati di configurazione delle risorse all'interno dell'aggregatore.

I primi dieci tipi di risorse per numero di risorse

Visualizza un grafico a barre orizzontali in cui vengono confrontati fino a dieci tipi di risorse dell'aggregatore selezionato, in ordine decrescente, in base al numero di risorse. Passa il mouse sul grafico per visualizzare il numero esatto di risorse per ogni tipo di risorsa.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato e dalle regioni in cui l'aggregatore selezionato è configurato per la raccolta dei dati.

Numero di risorse per regione

Visualizza un grafico a barre orizzontali in cui vengono confrontate fino a dieci regioni in cui l'aggregatore selezionato raccoglie i dati, in ordine decrescente, in base al numero di risorse. Passa il mouse sul grafico per visualizzare il numero esatto di risorse per ogni regione.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato.

I primi dieci account in base al numero di risorse

Visualizza un grafico a barre orizzontali in cui vengono confrontati fino a dieci account dell'aggregatore selezionato, in ordine decrescente, in base al numero di risorse. Passa il mouse sul grafico per visualizzare il numero esatto di risorse per ogni tipo di risorse.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato e dalle regioni in cui l'aggregatore selezionato è configurato per la raccolta dei dati.

Numero di risorse per tipi di risorse del servizio Amazon EC2

Visualizza un grafico a barre orizzontali in cui vengono confrontati i tipi di risorse Amazon EC2 dell'aggregatore selezionato, in ordine decrescente, in base al numero di risorse. Passa il mouse sul grafico per visualizzare il numero esatto di risorse per ogni tipo di risorse Amazon EC2.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato e dalle regioni in cui l'aggregatore selezionato è configurato per la raccolta dei dati. Per utilizzare questo grafico, occorre configurare il registratore sulla registrazione dei tipi di risorse Amazon EC2. Per ulteriori informazioni, consulta Selezione dei record di risorse. AWS Config

I primi dieci tipi di istanze EC2 utilizzati

Visualizza un grafico a barre orizzontali in cui vengono confrontati fino a dieci tipi di istanze Amazon EC2 dell'aggregatore selezionato, in ordine decrescente, in base all'uso. Passa il mouse sul grafico per vedere l'utilizzo per ogni tipo di istanza EC2.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato e dalle regioni in cui l'aggregatore selezionato è configurato per la raccolta dei dati. Per utilizzare questo grafico, occorre configurare il registratore sulla registrazione del tipo di risorse dell'istanza EC2. Per ulteriori informazioni, vedere Recoding Resources. AWS

Conteggi dei volumi EBS per tipo e dimensione del volume

Visualizza un grafico a barre verticali in cui vengono confrontati i volumi EBS dell'aggregatore selezionato in base al numero di risorse. Passa il mouse sul grafico per visualizzare nel dettaglio il numero e le dimensioni di ogni tipo di volume EBS.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato e dalle regioni in cui l'aggregatore selezionato è configurato per la raccolta dei dati. Per utilizzare questo grafico, occorre configurare il registratore sulla registrazione del tipo di risorsa del volume EC2. Per ulteriori informazioni, vedere Selezione dei record di risorse AWS Config.

Numero di istanze EC2 in esecuzione rispetto a quelle interrotte per tipo

Visualizza un grafico a barre orizzontali in cui vengono confrontati i tipi di istanze EC2 dell'aggregatore selezionato in esecuzione con le istanze EC2 interrotte per tipo di istanza. Passa il mouse sul grafico per vedere il numero esatto di istanze EC2 interrotte e in esecuzione per ogni tipo.

I dati visualizzati dipendono dalle impostazioni del registratore di configurazione per ogni account nell'aggregatore selezionato e dalle regioni in cui l'aggregatore selezionato è configurato per la raccolta dei dati. Per utilizzare questo grafico, occorre configurare il registratore sulla registrazione del tipo di risorse dell'istanza EC2. Per ulteriori informazioni, vedere Recoding Resources. AWS

Impostazione di un aggregatore utilizzando la Console

Nella pagina Aggregator (Aggregatore), segui questi passaggi:

- Crea un aggregatore specificando gli ID degli account o l'organizzazione di origine e le regioni da cui desideri aggregare i dati.
- Modifica ed elimina un aggregatore.

Argomenti

- Creazione di un aggregatore
- Modificare un aggregatore
- Eliminare un aggregatore

Creazione di un aggregatore

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Accedi alla pagina Aggregatori e scegli Crea aggregatore.
3. Consenti la replica dei dati, autorizza AWS Config a replicare i dati dagli account di origine in un account aggregatore.

   Scegli Consenti AWS Config per replicare i dati dagli account di origine in un account aggregatore. Devi selezionare questa casella di controllo per proseguire con l'aggiunta dell'aggregatore.
4. Alla voce Aggregator name (Nome aggregatore) digitare un nome per l'aggregatore.

   Il nome dell'aggregatore deve essere un nome univoco con una lunghezza massima di 64 caratteri alfanumerici. Il nome può contenere trattini e caratteri di sottolineatura.

5. Alla voce Select source accounts (Seleziona account di origine), scegliere Add individual account IDs (Aggiungi ID account singoli) o Add my organization (Aggiungi la mia organizzazione) per specificare le origini da cui si desidera aggregare i dati.

> **Note**
>
> L'autorizzazione è richiesta quando utilizzi Aggiungi singoli ID account per selezionare gli account di origine.

- Scegliendo Add individual account IDs (Aggiungi ID account singoli) è possibile aggiungere, a un account di aggregazione., degli ID account singoli.
  1. Scegliere Add source accounts (Aggiungi account di origine) per aggiungere gli ID account.
  2. Scegli Aggiungi Account AWS ID per aggiungere manualmente ID separati da Account AWS virgole. Se desideri aggregare i dati dall'account corrente, digita l'ID account dell'account stesso.

     O

     Scegli Carica un file per caricare un file (.txt o.csv) di ID separati da virgole. Account AWS
  3. Scegliere Add source accounts (Aggiungi account di origine) per confermare la selezione.
- Scegliendo Add my organization (Aggiungi la mia organizzazione), è possibile aggiungere, a un account di aggregazione, tutti gli account della propria organizzazione.

> **Note**
>
> Devi aver effettuato l'accesso all'account di gestione o a un account amministratore delegato registrato e devono essere abilitate nell'organizzazione tutte le funzionalità. Se il chiamante è un account di gestione, chiama l'API per abilitare l'integrazione tra e AWS Config . `EnableAwsServiceAccess` AWS Config AWS Organizations Se il chiamante è un amministratore delegato registrato, AWS Config chiama l'`ListDelegatedAdministratorsAPI` per verificare se il chiamante è un amministratore delegato valido.
> Assicurati che l'account di gestione registri l'amministratore delegato per il nome principale del AWS Config servizio (config.amazonaws.com) prima che

l'amministratore delegato crei un aggregatore. Per registrare un amministratore delegato, consulta Registrazione di un amministratore delegato.

Devi assegnare un ruolo IAM per consentire di chiamare API di sola lettura per la tua organizzazione. AWS Config

1. Scegli Scegli un ruolo dal tuo account per selezionare un ruolo IAM esistente.

> **Note**
>
> Nella console IAM, associa la policy `AWSConfigRoleForOrganizations` gestita al ruolo IAM. L'aggiunta di questa policy consente di AWS Config chiamare AWS Organizations `DescribeOrganization` e API. `ListAWSServiceAccessForOrganization` `ListAccounts` Per impostazione predefinita, `config.amazonaws.com` viene specificato automaticamente come entità attendibile.

2. Oppure, per creare un ruolo IAM, scegli Crea un ruolo e digita un nome per il tuo ruolo IAM.

6. Alla voce Regions (Regioni), scegliere le regioni per cui si desiderano aggregare i dati.
   - Seleziona una o più regioni o tutte le Regioni AWS.
   - Seleziona Includi futuro Regioni AWS per aggregare i dati di tutti i futuri Regioni AWS in cui è abilitata l'aggregazione di dati multi-account e più regioni.
7. Scegli Salva. AWS Config visualizza l'aggregatore.

Modificare un aggregatore

1. Per modificare l'aggregatore, scegli il nome dell'aggregatore.
2. Scegliere Actions (Operazioni), quindi scegliere Edit (Modifica).
3. Utilizza le sezioni della pagina Modifica aggregatore per modificare gli account di origine, i ruoli IAM o le regioni dell'aggregatore.

> **Note**
>
> Non è possibile modificare il tipo di origine da account singoli a organizzazione e viceversa.

4. Selezionare Salva.

Eliminare un aggregatore

1. Per eliminare un aggregatore, scegli il nome dell'aggregatore.
2. Scegliere Actions (Operazioni), quindi selezionare Delete (Elimina VPC).

   Viene visualizzato un messaggio di avviso. L'eliminazione di un aggregatore comporta la perdita di tutti i dati aggregati. Non è possibile ripristinare tali dati, ma i dati del/degli account di origine non sono intaccati.
3. Scegliere Delete (Elimina) per confermare la scelta.

Configurazione di un aggregatore utilizzando il AWS Command Line Interface

Puoi creare, visualizzare, aggiornare ed eliminare i dati AWS Config aggregatori utilizzando (). AWS Command Line Interface AWS CLI

AWS CLI È uno strumento unificato per gestire i tuoi AWS servizi. Con un solo strumento da scaricare e configurare, puoi controllare più AWS servizi dalla riga di comando e utilizzare script per automatizzarli. Per ulteriori informazioni sugli strumenti AWS CLI e per istruzioni sull'installazione degli AWS CLI strumenti, vedere quanto segue nella Guida per l'AWS Command Line Interface utente.

- AWS Command Line Interface Guida per l'utente
- Come configurare la AWS Command Line Interface

Se necessario, accedi `aws configure` per configurare l'utilizzo AWS CLI di una AWS regione in cui siano disponibili gli aggregatori.

Argomenti

- Aggiungi un aggregatore utilizzando account individuali
- Aggiunta di un aggregatore utilizzando AWS Organizations
- Registrazione di un amministratore delegato
- Visualizzare un aggregatore
- Modificare un aggregatore
- Eliminare un aggregatore

Aggiungi un aggregatore utilizzando account individuali

1. Apri un prompt dei comandi o una finestra del terminale.
2. Digitare il comando seguente per creare un aggregatore denominato **`MyAggregator`**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

   Per `account-aggregation-sources`, immetti uno dei seguenti valori.

   - Un elenco di Account AWS ID separati da virgole per i quali desideri aggregare i dati. Racchiudi l'ID account tra parentesi quadre e assicurati di fare l'escape delle virgolette (ad esempio, `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\", \"AccountID3\"],\"AllAwsRegions\": true}]"`).
   - Puoi anche caricare un file JSON di ID separati da virgole. Account AWS Caricare il file utilizzando la sintassi seguente: `--account-aggregation-sources MyFilePath/MyFile.json`

     Il file JSON deve avere il seguente formato:

```
[
    {
        "AccountIds": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ],
```

```
        "AllAwsRegions": true
    }
]
```

3. Premere Invio per eseguire il comando.

   Verrà visualizzato un output simile al seguente:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3"
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
    }
}
```

Aggiunta di un aggregatore utilizzando AWS Organizations

Prima di avviare questa procedura, devi aver effettuato l'accesso all'account di gestione o a un account amministratore delegato registrato e devono essere abilitate nell'organizzazione tutte le funzionalità.

> **Note**
>
> Assicurati che l'account di gestione registri un amministratore delegato con entrambi i seguenti nomi principali di AWS Config servizio (`config.amazonaws.comeconfig-multiaccountsetup.amazonaws.com`) prima che l'amministratore delegato crei un

aggregatore. Per registrare un amministratore delegato, consulta Registrazione di un amministratore delegato.

1. Apri un prompt dei comandi o una finestra del terminale.
2. Se non hai creato un ruolo IAM per il tuo AWS Config aggregatore, inserisci il seguente comando:

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"\",\"Effect\":\"Allow\",
\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action\":\"sts:AssumeRole
\"}]}" --description "Role for organizational AWS Config aggregator"
```

> **Note**
>
> Copia l'Amazon Resource Name (ARN) da questo ruolo IAM per utilizzarlo quando crei il tuo AWS Config aggregatore. Puoi trovare l'ARN nell'oggetto risposta.

3. Se non hai associato una policy al tuo ruolo IAM, collega la policy AWSConfigRoleForOrganizationsgestita o inserisci il seguente comando:

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAWSSe
```

4. Digitare il comando seguente per creare un aggregatore denominato **`MyAggregator`**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",
\"AllAwsRegions\": true}"
```

5. Premere Invio per eseguire il comando.

   Verrà visualizzato un output simile al seguente:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
```

```
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Registrazione di un amministratore delegato

Gli amministratori delegati sono account all'interno di una determinata AWS organizzazione a cui vengono concessi privilegi amministrativi aggiuntivi per un servizio specifico. AWS

1. Accedi con le credenziali dell'account di gestione.
2. Apri un prompt dei comandi o una finestra del terminale.
3. Immettete il comando seguente per abilitare l'accesso al servizio in qualità di amministratore delegato affinché l'organizzazione distribuisca e gestisca AWS Config regole e pacchetti di conformità in tutta l'organizzazione:

   ```
   aws organizations enable-aws-service-access --service-principal=config-
   multiaccountsetup.amazonaws.com
   ```

4. Immettete il seguente comando per abilitare l'accesso al servizio in qualità di amministratore delegato per consentire all'organizzazione di aggregare i dati AWS Config all'interno dell'organizzazione:

   ```
   aws organizations enable-aws-service-access --service-
   principal=config.amazonaws.com
   ```

5. Per verificare se l'abilitazione dell'accesso al servizio è completa, digita il comando seguente e premi Invio per eseguirlo.

   ```
   aws organizations list-aws-service-access-for-organization
   ```

   Verrà visualizzato un output simile al seguente:

   ```
   {
   ```

```
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
            "DateEnabled": 1607020860.881
        }
    ]
}
```

6. Digita quindi il comando seguente per registrare un account membro come amministratore delegato per AWS Config.

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

e

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. Per verificare se la registrazione dell'amministratore delegato è completa, digita il seguente comando dall'account di gestione e premi Invio per eseguirlo.

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

e

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

Verrà visualizzato un output simile al seguente:

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
            "Arn": "arn:aws:organizations::MemberAccountID:account/o-
c7esubdi38/MemberAccountID",
```

```
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
            "DelegationEnabledDate": 1607020986.801
        }
    ]
}
```

Visualizzare un aggregatore

1. Immetti il comando seguente:

```
aws configservice describe-configuration-aggregators
```

2. In base al tuo account di origine, dovrebbe essere visualizzato un output simile al seguente:

   Per account singoli

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "MyAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

O

Per un'organizzazione

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Modificare un aggregatore

1. Puoi utilizzare il comando `put-configuration-aggregator` per aggiornare o modificare un aggregatore di configurazioni.

   Per aggiungere un nuovo ID account a **`MyAggregator`** digita il comando seguente:

   ```
   aws configservice put-configuration-aggregator --configuration-aggregator-name
    MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
   \"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
   ```

2. In base al tuo account di origine, dovrebbe essere visualizzato un output simile al seguente:

   Per account singoli

   ```
   {
       "ConfigurationAggregator": {
           "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
   aggregator/config-aggregator-xz2upuu6",
           "CreationTime": 1517952090.769,
           "ConfigurationAggregatorName": "MyAggregator",
   ```

```
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

O

Per un'organizzazione

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Eliminare un aggregatore

Immetti il comando seguente:

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
 MyAggregator
```

In caso di esito positivo, il comando viene eseguito senza ulteriore output.

Autorizzazione degli account di aggregazione a raccogliere dati AWS Config di configurazione e conformità tramite la console

AWS Config consente di autorizzare gli account a raccogliere dati AWS Config di configurazione e conformità.

Nella pagina Authorizations (Autorizzazioni), segui questi passaggi:

- Aggiungi un'autorizzazione per consentire a un account e a una regione di un aggregatore specificato di raccogliere i dati di configurazione e conformità di AWS Config dall'account corrente.
- Autorizza una richiesta in sospeso dall'account di un aggregatore per raccogliere i dati di configurazione e conformità di AWS Config dall'account corrente.
- Elimina l'autorizzazione che consente a un aggregatore di raccogliere i dati di configurazione e conformità di AWS Config dall'account corrente.

Argomenti

- Considerazioni
- Aggiungi autorizzazione per gli account e le regioni degli aggregatori
- Autorizza una richiesta in sospeso per l'account di un aggregatore
- Eliminazione dell'autorizzazione per l'account di un aggregatore esistente

Considerazioni

Esistono due tipi di aggregatori: aggregatore di account individuali e aggregatore di organizzazioni

Per un aggregatore di account individuali, è richiesta l'autorizzazione per tutti gli account e le regioni di origine che desideri includere, inclusi gli account e le regioni esterni e gli account e le regioni membri dell'organizzazione.

Per un aggregatore di organizzazioni, l'autorizzazione non è richiesta per le aree degli account membri dell'organizzazione poiché l'autorizzazione è integrata nel AWS Organizations servizio.

Gli aggregatori non si attivano automaticamente per conto AWS Config dell'utente

AWS Config deve essere abilitato nell'account di origine e nella regione per entrambi i tipi di aggregatore, affinché AWS Config i dati vengano generati nell'account di origine e nella regione.

Aggiungi autorizzazione per gli account e le regioni degli aggregatori

È possibile aggiungere l'autorizzazione per concedere l'autorizzazione agli account aggregatori e alle regioni per raccogliere dati di AWS Config configurazione e conformità.

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Vai alla pagina Authorizations (Autorizzazioni) e seleziona Add authorization (Aggiungi autorizzazione).
3. Per l'Aggregator account (Account aggregatore), digita l'ID a 12 cifre dell'account di un aggregatore.
4. Per la regione Aggregator, scegli Regioni AWS dove l'account aggregatore può raccogliere i dati di configurazione e conformità di AWS Config.
5. Seleziona Aggiungi autorizzazione per confermare la selezione.

   AWS Config visualizza un account aggregatore, una regione e lo stato di autorizzazione.

   > **Note**
   >
   > Puoi anche aggiungere autorizzazioni agli account aggregatori e alle regioni in modo programmatico utilizzando modelli di esempio. AWS CloudFormation Per ulteriori informazioni, consulta la Guida AWS::Config::AggregationAuthorizationper l'AWS CloudFormation utente.

Autorizza una richiesta in sospeso per l'account di un aggregatore

Se è presente una richiesta di autorizzazione in sospeso dall'account di un aggregatore esistente, visualizzerai lo stato della richiesta nella pagina Autorizzazioni. È possibile autorizzare una richiesta in sospeso da questa pagina.

1. Scegli l'account dell'aggregatore che desideri autorizzare, quindi seleziona Autorizza.

   Viene visualizzato un messaggio di conferma per confermare che si desidera concedere all'account aggregatore l'autorizzazione a raccogliere AWS Config dati da questo account.

2. Seleziona nuovamente Autorizza per confermare che desideri concedere l'autorizzazione all'account dell'aggregatore.

   Lo stato di autorizzazione cambia da Requesting for authorization (Richiesta di autorizzazione) a Authorized (Autorizzato).

Periodo di approvazione dell'autorizzazione

L'approvazione dell'autorizzazione è necessaria per aggiungere gli account di origine all'aggregatore di account individuali. Le richieste di approvazione dell'autorizzazione in sospeso restano disponibili per 7 giorni dopo che un aggregatore di account individuali ha aggiunto un account di origine.

Eliminazione dell'autorizzazione per l'account di un aggregatore esistente

1. Scegli l'account dell'aggregatore per cui desideri eliminare l'autorizzazione, quindi seleziona Elimina.

   Viene visualizzato un messaggio di avviso. Quando elimini questa autorizzazione, AWS Config i dati non verranno più condivisi con l'account aggregatore.
2. Seleziona nuovamente Elimina per confermare la scelta.

   L'account dell'aggregatore è stato eliminato.

Dopo l'eliminazione dell'autorizzazione per un aggregatore, i dati rimangono nell'account dell'aggregatore per un massimo di 24 ore prima di essere eliminati.

Autorizzazione degli account di aggregazione alla raccolta dei dati AWS Config di configurazione e conformità utilizzando AWS Command Line Interface

Puoi autorizzare gli account aggregatori a raccogliere AWS Config dati dagli account di origine ed eliminare gli account aggregatori utilizzando (). AWS Command Line Interface AWS CLI Per utilizzare la console di AWS gestione, vedere. Autorizzazione degli account di aggregazione a raccogliere dati AWS Config di configurazione e conformità tramite la console

AWS CLI È uno strumento unificato per gestire i tuoi AWS servizi. Con un solo strumento da scaricare e configurare, puoi controllare più AWS servizi dalla riga di comando e utilizzare script per

automatizzarli. Per ulteriori informazioni sugli strumenti AWS CLI e per istruzioni sull'installazione degli AWS CLI strumenti, vedere quanto segue nella Guida per l'AWS Command Line Interface utente.

- AWS Command Line Interface Guida per l'utente
- Come configurare la AWS Command Line Interface

Se necessario, digitare `aws configure` per configurare l'utilizzo AWS CLI di una AWS regione in cui sono disponibili pacchetti di AWS Config conformità.

Argomenti

- Considerazioni
- Aggiungi autorizzazione per gli account e le regioni degli aggregatori
- Elimina un account di autorizzazione

Considerazioni

Esistono due tipi di aggregatori: aggregatore di account individuali e aggregatore di organizzazioni

Per un aggregatore di account individuali, è richiesta l'autorizzazione per tutti gli account e le regioni di origine che desideri includere, inclusi gli account e le regioni esterni e gli account e le regioni membri dell'organizzazione.

Per un aggregatore di organizzazioni, l'autorizzazione non è richiesta per le regioni degli account membri dell'organizzazione poiché l'autorizzazione è integrata nel servizio. AWS Organizations

Gli aggregatori non si attivano automaticamente per conto AWS Config dell'utente

AWS Config deve essere abilitato nell'account di origine e nella regione per entrambi i tipi di aggregatore, affinché AWS Config i dati vengano generati nell'account di origine e nella regione.

Aggiungi autorizzazione per gli account e le regioni degli aggregatori

1. Apri un prompt dei comandi o una finestra del terminale.
2. Immetti il comando seguente:

```
aws configservice put-aggregation-authorization --authorized-account-id  AccountID
 --authorized-aws-region Region
```

3. Verrà visualizzato un output simile al seguente:

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

Elimina un account di autorizzazione

Immetti il comando seguente:

```
aws configservice delete-aggregation-authorization --authorized-account-id  AccountID
 --authorized-aws-region Region
```

In caso di esito positivo, il comando viene eseguito senza ulteriore output.

Query dello stato di configurazione corrente delle risorse AWS

Presentazione di una funzionalità di anteprima per le query avanzate che consente di utilizzare le funzionalità di intelligenza artificiale generativa (AI generativa) per inserire istruzioni in un inglese semplice e convertirle in un formato di query. ready-to-use Per ulteriori informazioni, consulta Natural language interrogation processor for advanced query.

È possibile utilizzarle AWS Config per interrogare lo stato di configurazione corrente delle AWS risorse in base alle proprietà di configurazione per un singolo account e regione o per più account e regioni. È possibile eseguire query basate sulle proprietà sui metadati dello stato AWS delle risorse correnti su un elenco di risorse che supportano. AWS Config Per ulteriori risorse sull'elenco di tipi di risorsa supportati, consulta Tipi di risorsa supportati per query avanzate.

Le query avanzate forniscono un unico endpoint di query e un linguaggio di query per ottenere i metadati correnti sullo stato delle risorse senza eseguire chiamate API di descrizione specifiche del servizio. Puoi utilizzare gli aggregatori di configurazione per eseguire le stesse query da un account centrale su più account e regioni. AWS

Argomenti

- Funzionalità
- Componenti della query
- Query di esempio
- Esempi di query sulle relazioni
- Limitazioni
- Supporto nelle regioni
- Query con l'editor di query SQL (console)
- Query con l'editor di query SQL (AWS CLI)
- Natural language interrogation processor for advanced query.

Funzionalità

AWS Config utilizza un sottoinsieme della `SELECT` sintassi SQL (Structured Query Language) per eseguire query e aggregazioni basate sulle proprietà sui dati degli elementi di configurazione (CI) correnti. Le query variano in termini di complessità, da corrispondenze con identificatori di tag e/o risorse a query più complesse, come la visualizzazione di tutti i bucket Amazon S3 con il controllo delle versioni disabilitato. Ciò ti consente di eseguire esattamente la query dello stato corrente della risorsa di cui hai bisogno senza eseguire le chiamate API specifiche del servizio AWS .

Supporta le funzioni di aggregazione, ad esempio `AVG`, `COUNT`, `MAX`, `MIN` e `SUM`.

È possibile utilizzare le query avanzate per:

- Gestione dell'inventario, ad esempio per recuperare un elenco di istanze Amazon EC2 di dimensioni specifiche.
- Sicurezza e intelligenza operativa, ad esempio per recuperare un elenco di risorse che hanno una specifica proprietà di configurazione abilitata o disabilitata.
- Ottimizzazione dei costi, ad esempio per identificare un elenco di volumi Amazon EBS che non sono collegati a nessuna istanza EC2.
- Dati di conformità, ad esempio per recuperare un elenco di tutti i pacchetti di conformità e il relativo stato di conformità.

Per informazioni su come utilizzare AWS SQL Query Language, consulta What Is SQL (Structured Query Language)? .

Componenti della query

I componenti di query SQL `SELECT` sono indicati di seguito.

Riepilogo

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

Parametri

[condizione WHERE]

I filtri restituiscono risultati in base alla `condition` specificata.

[GROUP BY property]

Aggrega il set di risultati in gruppi di righe con valori corrispondenti per la proprietà specificata.

La clausola GROUP BY è applicabile alle aggregazioni.

[ORDER BY property [ASC | DESC] [, property [ASC | DESC] ...]]

Ordina un set di risultati da uno o più output `properties`.

Quando la clausola contiene più proprietà, il set di risultati viene ordinato in base alla prima `property`, quindi in base alla seconda `property` per le righe che hanno valori corrispondenti per la prima proprietà e così via.

Esempi

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

Query di esempio

Query to list all EC2 instances with AMI ID ami-12345

Query:

```
SELECT
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
```

```
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

Risultati:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
                "Name": "configuration.placement.tenancy"
            },
            {
                "Name": "configuration.imageId"
            },
            {
                "Name": "availabilityZone"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
```

```
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}"
    ]
}
```

Query for count of resources grouped by their AWS Config rules compliance status

Query:

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
    configuration.complianceType
```

Risultati:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

Query for the compliance status of AWS Conformance packs

Query:

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

Risultati:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.complianceType"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

Query to get counts of AWS resources grouped by account ID

Query:

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

Risultati:

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
            {
                "Name": "accountId"
            }
        ]
    }
}
```

Query to list all EC2 volumes that are not in use

Query:

```
SELECT
    resourceId,
    accountId,
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
```

```
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

Risultati:


```
{
    "Results": [
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "accountId"
            },
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
```

```
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
            },
            {
                "Name": "configuration.availabilityZone"
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
}
```

Esempi di query sulle relazioni

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

O

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

Limitazioni

> **Note**
>
> L'interrogazione avanzata non supporta l'interrogazione di risorse che non sono state configurate per essere registrate dal registratore di configurazione. AWS Config crea elementi di configurazione (CI) con `ResourceNotRecorded` in `configurationItemStatus` quando una risorsa è stata scoperta ma non è configurata per essere registrata dal registratore di configurazione. Sebbene un aggregatore aggreghi questi CI, la query avanzata non supporta le query sui CI con `ResourceNotRecorded`. Aggiorna le impostazioni del registratore per abilitare la registrazione dei tipi di risorse su cui eseguire le query.

Come sottoinsieme di SQL `SELECT`, la sintassi di query ha le limitazioni seguenti:

- In una query non sono supportate le parole chiave `ALL`, `AS`, `DISTINCT`, `FROM`, `HAVING`, `JOIN` e `UNION`. Le query con valore `NULL` non sono supportate.
- Non sono supportate query su risorse di terze parti. Per le risorse di terze parti recuperate utilizzando query avanzate, il campo di configurazione sarà impostato su `NULL`.
- Non sono supportate strutture annidate (come i tag) da decomprimere con le query SQL.
- La notazione CIDR viene convertita in intervalli IP per la ricerca. Ciò significa che `"="` e `"BETWEEN"` cercano qualsiasi intervallo che includa l'IP fornito, anziché uno esatto. Per cercare un intervallo IP esatto, è necessario aggiungere ulteriori condizioni per escludere gli IP al di fuori dell'intervallo. Ad esempio, per cercare 10.0.0.0/24 e solo quel blocco IP, puoi eseguire:

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
```

```
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

Per 192.168.0.2/32, puoi effettuare la ricerca in modo simile:

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

- Quando esegui query su più proprietà all'interno di un array di oggetti, le corrispondenze vengono calcolate su tutti gli elementi dell'array. Ad esempio, per una risorsa R con le regole A e B, la risorsa è conforme alla regola A ma non conforme alla regola B. La risorsa R viene archiviata come:

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

La risorsa R verrà restituita da questa query:

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

La prima condizione `configuration.configRuleList.complianceType = 'non_compliant'` viene applicata a TUTTI gli elementi in R.configRuleList, poiché R ha una regola (regola B) con complianceType = 'non_compliant', la condizione viene valutata come vera. La seconda condizione `configuration.configRuleList.configRuleName` viene applicata a TUTTI gli elementi in R.configRuleList, poiché R ha una regola (regola A) con configRuleName = 'A', la condizione viene valutata come vera. Poiché entrambe le condizioni sono true, verrà restituita la risorsa R.

- Il formato abbreviato `SELECT` per tutte le colonne (cioè `SELECT *`) seleziona solo le proprietà scalari di livello superiore di un elemento di configurazione. Le proprietà scalari restituite sono `accountId`, `awsRegion`, `arn`, `availabilityZone`, `configurationItemCaptureTime`, `resourceCreationTime`, `resourceId`, `resourceName`, `resourceType` e `version`.
- Limitazioni dei caratteri jolly:
  - I caratteri jolly sono supportati solo per i valori di proprietà e non per le chiavi di proprietà (ad esempio, `...WHERE someKey LIKE 'someValue%'` è supportato, mentre `...WHERE 'someKey%' LIKE 'someValue%'` non è supportato).
  - Supporto solo per caratteri jolly suffisso (ad esempio, `...LIKE 'AWS::EC2::%'` e `...LIKE 'AWS::EC2::_'` sono supportati, mentre `...LIKE '%::EC2::Instance'` e `...LIKE '_::EC2::Instance'` non sono supportati).
  - Le corrispondenze con caratteri jolly devono contenere almeno tre caratteri (ad esempio, `...LIKE 'ab%'` e `...LIKE 'ab_'` non sono consentiti, mentre `...LIKE 'abc%'` e `...LIKE 'abc_'` sono consentiti).

> **Note**
>
> Anche il carattere "_" (trattino basso singolo) viene considerato come un carattere jolly.

- Limitazioni delle aggregazioni:
  - Le funzioni di aggregazione possono accettare un solo argomento o una sola proprietà.
  - Le funzioni di aggregazione non possono accettare altre funzioni come argomenti.
  - `GROUP BY` con una clausola `ORDER BY` che fa riferimento a funzioni aggregate può contenere una sola proprietà.
  - Per tutte le altre aggregazioni, le clausole `GROUP BY` possono contenere fino a tre proprietà.
  - L'impaginazione è supportata per tutte le query aggregate tranne quando la clausola `ORDER BY` ha una funzione di aggregazione. Ad esempio, `GROUP BY X, ORDER BY Y` non funziona se `Y` è una funzione di aggregazione.
  - Nessun supporto per le clausole `HAVING` nelle aggregazioni.
- Limitazioni degli identificatori non corrispondenti:

  Gli identificatori non corrispondenti sono proprietà che hanno la stessa ortografia ma lettere maiuscole e minuscole diverse. La query avanzata non supporta l'elaborazione di query che contengono identificatori non corrispondenti. Per esempio:

- Due proprietà con la stessa ortografia ma con lettere maiuscole e minuscole diverse (`configuration.dbclusterIdentifier` e `configuration.dBClusterIdentifier`).
- Due proprietà in cui una proprietà è un sottoinsieme dell'altra e hanno lettere maiuscole e minuscole diverse (`configuration.ipAddress` e `configuration.ipaddressPermissions`).

Supporto nelle regioni

Le query avanzate sono supportate nelle seguenti regioni geografiche:

Nome della regione	Regione	Endpoint	Protocollo
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Stati Uniti occidentali (California settentrionale)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pacific (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asia Pacifico (Giacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asia Pacifico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacifico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacifico (Osaka-Locale)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacifico (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacifico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Centrale)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Canada occidentale (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Francoforte)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londra)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milano)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Europa (Parigi)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spagna)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zurigo)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israele (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Medio Oriente (Bahrein)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Medio Oriente (Emirati Arabi Uniti)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Sud America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Query con l'editor di query SQL (console)

Presentazione di una funzionalità di anteprima per le query avanzate che consente di utilizzare le funzionalità di intelligenza artificiale generativa (AI generativa) per inserire istruzioni in un inglese semplice e convertirle in un formato di query. ready-to-use Per ulteriori informazioni, consulta Natural language interrogation processor for advanced query.

È possibile utilizzare query di AWS esempio oppure creare query personalizzate denominate query personalizzate.

Considerazioni

Prerequisiti

Se utilizzi una delle seguenti politiche AWS gestite, avrai le autorizzazioni necessarie per eseguire e salvare una query: AWSServiceRoleForConfig(service-linked role) o AWS_. ConfigRole

Altrimenti, è necessario che le autorizzazioni siano incluse nella politica gestita. AWSConfigUserAccess AWS

Elenco di proprietà su cui è possibile interrogare

Un elenco aggiornato delle proprietà e dei relativi tipi di dati è disponibile in GitHub.

Interrogazioni e aggregatori avanzati

Per eseguire una query su un aggregatore, creare un aggregatore. Per ulteriori informazioni, consulta Impostazione di un aggregatore utilizzando la Console.

Se si dispone già di un aggregatore configurato, nell'ambito della query, scegliere l'aggregatore per eseguire una query avanzata su tale aggregatore. Quando selezioni un aggregatore, valuta la possibilità di aggiungere l' Account AWS ID e la AWS regione nell'istruzione di query per visualizzare tali informazioni nei risultati.

Usa una query di AWS esempio

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Scegliere Query avanzate dalla navigazione a sinistra per eseguire query sulle configurazioni delle risorse per un singolo account e regione o per più account e regioni.
3. Nella pagina Query avanzate, scegli una query appropriata dall'elenco delle query. Puoi filtrare l'elenco di query in base al nome, alla descrizione, all'autore o ai tag. Per filtrare le query AWS , scegli Creator e inserisci AWS. La query selezionata viene visualizzata nell'editor di query SQL. È possibile modificare la query selezionata in base alle proprie esigenze.
4. Per salvare questa query in una nuova, scegli Salva con nome.
   - Nel campo Nome della query, aggiorna il nome della query.
   - Nel campo Descrizione, aggiorna la descrizione della query.
   - Inserisci fino a 50 tag univoci per questa query.
   - Selezionare Salva.
5. Seleziona Esegui. I risultati della query vengono visualizzati nella tabella sotto l'editor di query.
6. Scegliere Esporta come per esportare i risultati della query in formato CSV o JSON.

> **Note**
>
> I risultati della query sono impaginati. Quando si sceglie l'esportazione, vengono esportati fino a 500 risultati.

È inoltre possibile utilizzare le API per recuperare tutti i risultati. I risultati sono impaginati ed è possibile recuperare 100 risultati alla volta.

Creazione di una query personalizzata

1. Accedi a AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Scegliere Query avanzate dalla navigazione a sinistra per eseguire query sulle configurazioni delle risorse per un singolo account e regione o per più account e regioni.
3. Per creare una query personalizzata, scegli Nuova query.

   Puoi visualizzare o modificare una query personalizzata in base al nome, alla descrizione, all'autore o ai tag. Per filtrare le query personalizzate, scegli Crea e inserisci Personalizzata.
4. Nella pagina Editor di query, crea la query personalizzata per l'account e l'area geografica. È inoltre possibile selezionare un aggregatore appropriato per creare una query per più account e regioni.
5. Scegli Modifica se vuoi apportare modifiche a questa query. Per salvare questa query, scegli Salva.
   - Nel campo Nome della query, aggiorna il nome della query.
   - Nel campo Descrizione, aggiorna la descrizione della query.
   - Inserisci fino a 50 tag univoci per questa query.
   - Selezionare Salva.
6. Seleziona Esegui. I risultati della query vengono visualizzati nella tabella sotto l'editor di query.
7. Scegliere Esporta come per esportare i risultati della query in formato CSV o JSON.

   I risultati della query sono impaginati. Quando si sceglie l'esportazione, vengono esportati fino a 500 risultati.

   È inoltre possibile utilizzare le API per recuperare tutti i risultati. I risultati sono impaginati ed è possibile recuperare 100 risultati alla volta.

Query con l'editor di query SQL (AWS CLI)

AWS CLI È uno strumento unificato per gestire i tuoi AWS servizi. Con un solo strumento da scaricare e configurare, puoi controllare più AWS servizi dalla riga di comando e utilizzare script per automatizzarli. Per ulteriori informazioni sugli strumenti AWS CLI e per istruzioni sull'installazione degli AWS CLI strumenti, vedere quanto segue nella Guida per l'AWS Command Line Interface utente.

- AWS Command Line Interface Guida per l'utente
- Come configurare la AWS Command Line Interface

Se necessario, accedi `aws configure` per configurare l'utilizzo AWS CLI di una AWS regione in cui sono disponibili interrogazioni avanzate.

Considerazioni

Prerequisiti

Se utilizzi una delle seguenti politiche AWS gestite, avrai le autorizzazioni necessarie per eseguire e salvare una query: AWSServiceRoleForConfig(service-linked role) o AWS_. ConfigRole

Altrimenti, è necessario che le autorizzazioni siano incluse nella politica gestita. AWSConfigUserAccess AWS

Elenco di proprietà su cui è possibile interrogare

Un elenco aggiornato delle proprietà e dei relativi tipi di dati è disponibile in GitHub.

Interrogazioni e aggregatori avanzati

Per eseguire una query su un aggregatore, creare un aggregatore. Per ulteriori informazioni, consulta Impostazione di un aggregatore utilizzando la Console.

Se si dispone già di un aggregatore configurato, nell'ambito della query, scegliere l'aggregatore per eseguire una query avanzata su tale aggregatore. Quando selezioni un aggregatore, valuta la possibilità di aggiungere l' Account AWS ID e la AWS regione nell'istruzione di query per visualizzare tali informazioni nei risultati.

Query sui dati di configurazione delle risorse

Per eseguire query sui dati di configurazione delle risorse utilizzando l'editor di query (AWS CLI) per un singolo account e regione

1. Apri un prompt dei comandi o una finestra del terminale.
2. Immettete il comando seguente per interrogare i dati di configurazione delle risorse.

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

A seconda della query, l'output ha il seguente aspetto:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

Per eseguire query sui dati di configurazione delle risorse utilizzando l'editor di query (AWS CLI) per più account e aree geografiche

1. Apri un prompt dei comandi o una finestra del terminale.
2. Immettete il comando seguente per interrogare i dati di configurazione delle risorse.

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

A seconda della query, l'output ha il seguente aspetto:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

> **Note**
>
> Durante l'utilizzo dei tipi di `AWS::IAM::Policy` risorse `AWS::IAM::User` `AWS::IAM::GroupAWS::IAM::Role`,, e in una query avanzata, utilizzare`awsRegion = 'global'`.

Salvataggio di una query

1. Apri un prompt dei comandi o una finestra del terminale.
2. Immettete il seguente comando per salvare una query.

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
```

```
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. A seconda della query, l'output ha il seguente aspetto:

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> `--tags` è facoltativo. Quando passi i tag, i tag salvati non vengono restituiti né da `list-stored-queries` né da `get-stored-query`. Per recuperare i tag associati a una query salvata, è necessario utilizzare `list-tag-for-resources`.
> `--description` è facoltativo durante la creazione o l'aggiornamento di una query.

Visualizzazione di tutte le query salvate

1. Immettere il comando seguente per visualizzare l'elenco di tutte le interrogazioni salvate.

```
aws configservice list-stored-queries
```

2. A seconda della query, l'output ha il seguente aspetto:

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
```

```
    ]
}
}
```

Recupero dei dettagli di una query salvata

1. Immettete il seguente comando per ottenere i dettagli di una specifica interrogazione salvata.

```
aws configservice get-stored-query --query-name cli-test
```

2. A seconda della query, l'output ha il seguente aspetto:

```
{
    "StoredQuery": {
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
        "Description": "cli test query",
        "Expression": "SELECT *"
    }
}
```

Eliminazione di una query salvata

- Immettete il seguente comando per eliminare l'interrogazione salvata.

```
aws configservice delete-stored-query --query-name cli-test
```

In caso di esito positivo, il comando viene eseguito senza ulteriore output.

Natural language interrogation processor for advanced query.

Il processore di query in linguaggio naturale per le query avanzate è in versione di anteprima AWS Config ed è soggetto a modifiche.

Il processore di query in linguaggio naturale per query avanzate utilizza Amazon Bedrock, una tecnologia di intelligenza artificiale generativa (AI generativa) che consente di inserire istruzioni in un inglese semplice e convertirle in un formato di query. ready-to-use Con il processore di interrogazioni in linguaggio naturale, puoi interrogare la tua o l'intera organizzazione. Account AWS AWS

Un prompt può essere una domanda o una dichiarazione. Ad esempio, puoi inserire richieste come «Quali sistemi di bilanciamento del carico vengono creati dopo il 1° gennaio 2024?» e «Elenca tutte le mie funzioni lambda che esegue node js 16".

Considerazioni

Il processore di query in linguaggio naturale non può eseguire le seguenti azioni:

- Genera query da lingue diverse dall'inglese.
- Genera interrogazioni da prompt che non si riferiscono a interrogazioni avanzate.
- Genera interrogazioni da prompt con più di 1000 caratteri.
- Genera domande a partire da correzioni successive o da sessioni precedenti.
- Spiega il codice che è stato generato.

Esegui query utilizzando il processore di query in linguaggio naturale

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Scegliere Query avanzate dalla navigazione a sinistra per eseguire query sulle configurazioni delle risorse per un singolo account e regione o per più account e regioni.
3. Nella pagina Interrogazioni avanzate, scegli Nuova query per accedere all'editor di query.
   - (Facoltativo) Per eseguire una query su un aggregatore, crea un aggregatore. Per ulteriori informazioni, consulta Impostazione di un aggregatore utilizzando la Console.
   - Se si dispone già di un aggregatore configurato, nell'ambito della query, scegliere l'aggregatore per eseguire una query avanzata su tale aggregatore. Quando selezioni un aggregatore, valuta la possibilità di aggiungere l' Account AWS ID e la AWS regione nell'istruzione della query per visualizzare tali informazioni nei risultati.
4. Nell'editor di Query, vai alla sezione Natural language Query Processor. Inserisci un prompt in un inglese semplice, quindi scegli Genera. Per esempi, consulta Prompt di esempio.

5. Dopo aver generato una query, puoi scegliere Copia (funzionalmente equivalente a Ctrl+C) per copiare la query negli appunti oppure scegliere Compila nell'editor. Se inserita nell'editor, è possibile modificare la query generata in base alle proprie esigenze.
6. Per salvare questa query in una nuova, scegli Salva con nome.
   - Nel campo Nome della query, aggiorna il nome della query.
   - Nel campo Descrizione, aggiorna la descrizione della query.
   - Inserisci fino a 50 tag univoci per questa query.
   - Selezionare Salva.
7. Seleziona Esegui. I risultati della query vengono visualizzati nella tabella sotto l'editor di query.
8. Scegliere Esporta come per esportare i risultati della query in formato CSV o JSON.

> **Note**
>
> I risultati della query sono impaginati. Quando si sceglie l'esportazione, vengono esportati fino a 500 risultati.
> È inoltre possibile utilizzare le API per recuperare tutti i risultati. I risultati sono impaginati ed è possibile recuperare 100 risultati alla volta.

Istruzioni di esempio

Di seguito sono riportati i prompt e le query di generazione che è possibile utilizzare come esempi.

Example: Quali sistemi di bilanciamento del carico sono stati creati dopo il 1° gennaio 2024?

Richiesta: What load balancers were created after January 1, 2024?

Interrogazione generata:

```
SELECT
    resourceId,
    resourceType,
    resourceCreationTime
WHERE
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
```

```
ORDER BY
    resourceCreationTime
DESC
```

Example: Quali delle mie istanze di database RDS sono accessibili pubblicamente?

Richiesta: Which of my RDS database instances are publicly accessible?

Interrogazione generata:

```
SELECT
    resourceId,
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: Quante istanze EC2 sono state create nell'ultimo anno?

Richiesta: How many EC2 instances were created in last one year?

Interrogazione generata:

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
    '2023-05-10T16:56:25.000Z'
AND
    '2024-05-10T16:56:25.000Z'
```

Example: Quante istanze EC2 ho in ognuna delle mie? Account AWS

Richiesta: How many EC2 instances do I have in each of my Account AWS?

Interrogazione generata:

```
SELECT
```

```
    accountId,
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: A quali ruoli IAM è AdministratorAccess allegata la policy gestita?

Richiesta: Which IAM roles have the managed policy AdministratorAccess attached?

Interrogazione generata:

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: Volumi EBS senza crittografia

Richiesta: EBS volumes without encryption

Interrogazione generata:

```
SELECT
    accountId
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.encrypted = false
```

Example: Ottieni risorse non conformi

Richiesta: Get noncompliant resources

Interrogazione generata:

```
SELECT
    resourceId,
```

```
    resourceType
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: Elenca tutte le mie funzioni lambda che esegue node js 16

Richiesta: List all my lambda function that is running node js 16

Interrogazione generata:

```
SELECT
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: Quali certificati ACM scadono nei prossimi 30 giorni?

Richiesta: What ACM certificates expire the next 30 days?

Interrogazione generata:

```
SELECT
    resourceId,
    configuration.domainName,
    configuration.notAfter
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
BETWEEN
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53’
```

> **Note**
>
> I tempi della query generata dipendono dall'ora in cui si immette il prompt.

Fornire un feedback

È possibile fornire un feedback generale sul processore di query in linguaggio naturale o un feedback su una specifica query generata.

Fornire feedback sul processore di interrogazioni in linguaggio naturale

Scegli il pulsante Fornisci feedback che appare sopra il processore di interrogazioni in linguaggio naturale a destra. Puoi inserire la tua soddisfazione o insoddisfazione e fornire un feedback su come AWS Config rendere più utile la query in linguaggio naturale.

> **Note**
>
> Non divulgate informazioni personali, commercialmente sensibili o riservate.

Fornire feedback su una specifica richiesta generata

Puoi fornire il tuo feedback su una query generata scegliendo il pulsante pollice su o pollice giù che appare sotto la query generata.

Supporto nelle regioni

Il processore di interrogazione in linguaggio naturale è supportato nelle seguenti regioni.

Nome della regione	Regione	Endpoint	Protocollo
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Eliminazione dei dati AWS Config

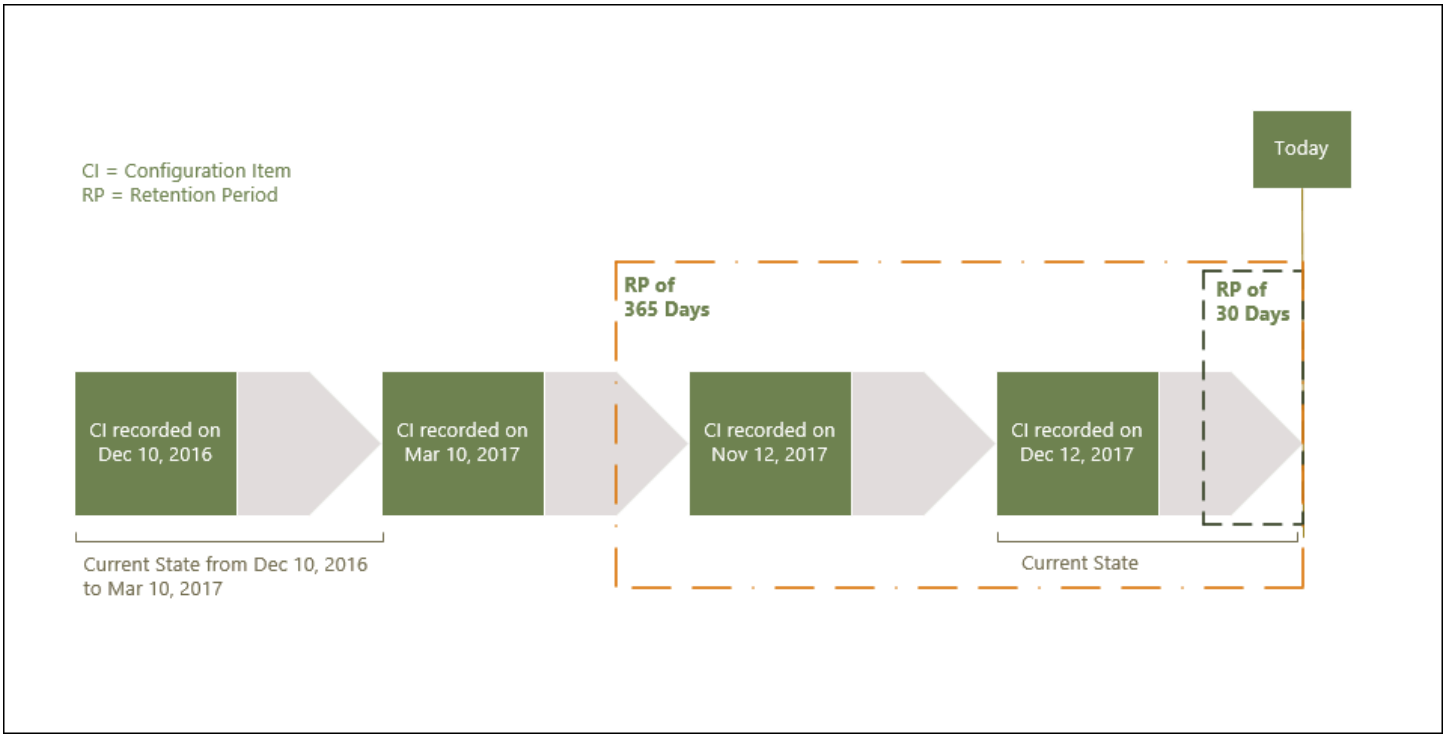
> **Note**
>
> Sebbene AWS Config utilizzi Amazon Simple Storage Service (Amazon S3) e Amazon Simple Notification Service (Amazon SNS) per l'invio di istantanee di configurazione e file di AWS Config cronologia di configurazione, dispone di proprie politiche di archiviazione e conservazione dei dati. Le informazioni in questa pagina sono specifiche per. AWS Config Amazon S3 e Amazon SNS hanno policy di archiviazione e conservazione dei dati separate.

AWS Config ti consente di eliminare i tuoi dati specificando un periodo di conservazione per il tuo`ConfigurationItems`. Quando specifichi un periodo di conservazione, AWS Config conserva il tuo `ConfigurationItems` per quel periodo specificato. Puoi scegliere un periodo compreso tra un minimo di 30 giorni e un massimo di 7 anni (2557 giorni). AWS Config elimina i dati più vecchi del periodo di conservazione specificato. Se non specifichi un periodo di conservazione, AWS Config continuerà ad archiviare `ConfigurationItems` per il periodo predefinito di 7 anni (2557 giorni). Se la registrazione è attivata, lo stato corrente della risorsa viene calcolato dal momento della registrazione del `ConfigurationItem`, fino a quando non viene registrata la modifica successiva (un nuovo `ConfigurationItem`).

Per comprendere il funzionamento del periodo di conservazione è sufficiente osservare la timeline.

- Quando la registrazione è attivata, lo stato corrente di una risorsa è sempre esistente e non può eliminato indipendentemente dalla data di registrazione del `ConfigurationItem`.
- Quando AWS Config i record sono nuovi`ConfigurationItems`, i precedenti `ConfigurationItems` vengono eliminati in base al periodo di conservazione specificato.

Nella sequenza temporale seguente, AWS Config i record `ConfigurationItems` nelle seguenti date. Nella timeline di esempio, il giorno odierno viene indicato come 24 maggio 2018.



La tabella seguente mostra quali `ConfigurationItems` sono visualizzati nella AWS Config timeline in base al periodo di conservazione selezionato.

Periodo di retention	Elementi di configurazione visualizzati nella timeline	Spiegazione
30 giorni	12 dicembre 2017	Lo stato corrente della risorsa inizia il 12 dicembre 2017 quando il `ConfigurationItem` è stato registrato e rimane valido fino alla data odierna (24 maggio 2018). Finché la registrazione è attiva, lo stato attuale è sempre esistente.
365 giorni	12 dicembre 2017; 12 novembre 2017 e 10 marzo 2017	Il periodo di conservazione mostra lo stato attuale, 12 dicembre 2017, e i `ConfigurationItems` precedenti del 12 novembre 2017 e 10 marzo 2017.

Periodo di retention	Elementi di configurazione visualizzati nella timeline	Spiegazione
		Il `ConfigurationItem` del 10 marzo 2017 viene visualizzato sulla timeline perché rappresenta lo stato di configurazione che era corrente nei 365 giorni precedenti.

Dopo aver specificato un periodo di conservazione, non vengono più restituite le AWS Config API `ConfigurationItems` che rappresentano uno stato precedente al periodo di conservazione specificato.

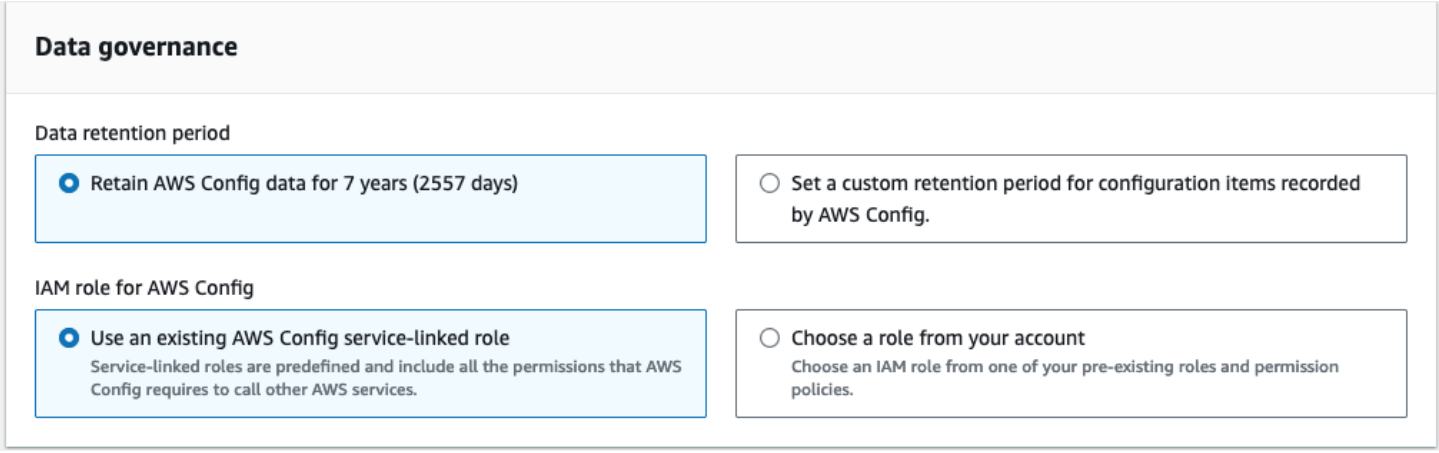
> **Note**
>
> - AWS Config non è possibile registrare il proprio `ConfigurationItems` se la registrazione è disattivata.
> - AWS Config non puoi registrare il tuo `ConfigurationItems` se il tuo ruolo IAM ha autorizzazioni insufficienti. Per ulteriori informazioni, consulta Autorizzazioni per il ruolo IAM assegnato a. AWS Config

Impostazione del periodo di conservazione dei dati in AWS Management Console

In AWS Management Console, se non si seleziona un periodo di conservazione dei dati, il periodo predefinito è 7 anni o 2557 giorni.

Per personalizzare il periodo di conservazione dei dati per gli elementi di configurazione seleziona la casella di controllo. Puoi indicare 1 anno, 3 anni, 5 anni oppure scegliere un periodo personalizzato. In quest'ultimo caso, inserisci un numero di giorni compreso tra 30 e 2557.

L'immagine seguente mostra dove è possibile impostare il periodo di conservazione dei dati in Data Governance. Puoi accedere a Data Governance dalla pagina Modifica impostazioni dalla AWS Config console scegliendo Impostazioni nella barra di navigazione a sinistra, quindi scegliendo Modifica.


Data governance
Data retention period
Retain AWS Config data for 7 years (2557 days)
Set a custom retention period for configuration items recorded by AWS Config.
IAM role for AWS Config
Use an existing AWS Config service-linked role
Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services.
Choose a role from your account
Choose an IAM role from one of your pre-existing roles and permission policies.

Sicurezza in AWS Config

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per informazioni sui programmi di conformità applicabili AWS Config, consulta i servizi in Scope by Compliance Program (AWSAWS servizi in Scope).
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Config. I seguenti argomenti mostrano come eseguire la configurazione AWS Config per soddisfare gli obiettivi di sicurezza e conformità.

Argomenti

- Protezione dei dati in AWS Config
- Identity and Access Management per AWS Config
- Risposta agli incidenti in AWS Config
- Convalida della conformità per AWS Config
- Resilienza in AWS Config
- Sicurezza dell'infrastruttura in AWS Config
- Prevenzione del confused deputy tra servizi
- Best practice di sicurezza per AWS Config

Protezione dei dati in AWS Config

Il modello di responsabilità AWS condivisa modello di si applica alla protezione dei dati in AWS Config. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutto il Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con AWS Config o altro Servizi AWS utilizzando la console, l'API o AWS gli AWS CLI SDK. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati a riposo

I dati vengono crittografati a riposo utilizzando la crittografia lato server trasparente. Questo consente di ridurre gli oneri operativi e la complessità associati alla protezione dei dati sensibili. La crittografia dei dati inattivi consente di creare applicazioni sicure che rispettano rigorosi requisiti normativi e di conformità per la crittografia.

Crittografia dei dati in transito

I dati raccolti e a cui accede AWS Config avvengono esclusivamente su un canale protetto Transport Layer Security (TLS).

Identity and Access Management per AWS Config

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS Config IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come AWS Config funziona con IAM
- Esempi di policy basate sull'identità per AWS Config
- AWS politiche gestite per AWS Config
- Autorizzazioni per il ruolo IAM assegnato a AWS Config
- Aggiornamento del ruolo IAM assegnato a AWS Config
- Autorizzazioni per il bucket Amazon S3 per il canale di distribuzione AWS Config
- Autorizzazioni per la chiave KMS per il AWS Config canale di consegna
- Autorizzazioni per l'argomento Amazon SNS
- Risoluzione dei problemi AWS Config di identità e accesso

- Utilizzo dei ruoli collegati ai servizi per AWS Config

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AWS Config svolgi.

Utente del servizio: se utilizzi il AWS Config servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS Config funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS Config, consulta Risoluzione dei problemi AWS Config di identità e accesso.

Amministratore del servizio: se sei responsabile delle AWS Config risorse della tua azienda, probabilmente hai pieno accesso a AWS Config. È tuo compito determinare a quali AWS Config funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS Config, consultaCome AWS Config funziona con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AWS Config. Per visualizzare esempi di policy AWS Config basate sull'identità che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per AWS Config

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWSnella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di

utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene

autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli

collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come AWS Config funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Config, scopri con quali funzionalità IAM è disponibile l'uso AWS Config.

Funzionalità IAM che puoi utilizzare con AWS Config

Funzionalità IAM	AWS Config supporto
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una panoramica di alto livello su come AWS Config e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per AWS Config

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di politiche basate sull'identità per AWS Config

Per visualizzare esempi di politiche basate sull' AWS Config identità, vedere. Esempi di policy basate sull'identità per AWS Config

Politiche basate sulle risorse all'interno AWS Config

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste

ulteriori policy basate su identità. Per ulteriori informazioni, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Azioni politiche per AWS Config

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di AWS Config azioni, vedere Azioni definite da AWS Config nel Service Authorization Reference.

Le azioni politiche in AWS Config uso utilizzano il seguente prefisso prima dell'azione:

```
config
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "config:action1",
      "config:action2"
         ]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "config:Describe*"
```

Per visualizzare esempi di politiche AWS Config basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Config

Risorse politiche per AWS Config

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di AWS Config risorse e dei relativi ARN, consulta Resources defined by AWS Config nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da AWS Config.

Per visualizzare esempi di politiche AWS Config basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Config

Chiavi relative alle condizioni delle politiche per AWS Config

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco di chiavi di AWS Config condizione, consulta Condition keys for AWS Config nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi Azioni definite da AWS Config.

Per visualizzare esempi di politiche AWS Config basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Config

ACL in AWS Config

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con AWS Config

Supporta ABAC (tag nelle policy)	Sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente IAM.

Per ulteriori informazioni sul tagging delle risorse di AWS Config , consulta Tagging delle risorse AWS Config.

Utilizzo di credenziali temporanee con AWS Config

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-On (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per AWS Config

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.

Ruoli di servizio per AWS Config

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. AWS Config Modifica i ruoli di servizio solo quando viene AWS Config fornita una guida in tal senso.

Ruoli collegati ai servizi per AWS Config

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli AWS Config collegati ai servizi, consulta. Utilizzo dei ruoli collegati ai servizi per AWS Config

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per AWS Config

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AWS Config . Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o l'API. AWS Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS Config, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione AWS Config nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Iscriviti per un Account AWS
- Crea un utente con accesso amministrativo

- Utilizzo della console di AWS Config
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Accesso in sola lettura a AWS Config
- Accesso completo a AWS Config
- Autorizzazioni supportate a livello di risorsa per le azioni dell'API Rule AWS Config
- Autorizzazioni a livello di risorsa supportate per l'aggregazione dei dati multi-regione multi-account

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare AWS Config risorse nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100

controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente IAM.

- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center

2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Utilizzo della console di AWS Config

Per accedere alla AWS Config console, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle AWS Config risorse del tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la AWS Config console, allega anche la policy AWS Config `AWSConfigUserAccess` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

È necessario concedere agli utenti le autorizzazioni con AWS Config cui interagire. Per gli utenti che necessitano dell'accesso completo a AWS Config, utilizza la policy Accesso completo alla politica AWS Config gestita.

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .
- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.
- Utenti IAM:

- Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Accesso in sola lettura a AWS Config

L'esempio seguente mostra una policy AWS gestita `AWSConfigUserAccess` che concede l'accesso in sola lettura a. AWS Config

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

Nelle istruzioni della policy, l'elemento `Effect` specifica se le operazioni sono consentite o negate. L'elemento `Action` elenca le operazioni specifiche che l'utente è autorizzato a eseguire. L'elemento `Resource` elenca le risorse AWS su cui l'utente è autorizzato a eseguire tali operazioni. Per le politiche che controllano l'accesso alle AWS Config azioni, l'`Resource`elemento è sempre impostato su`*`, un carattere jolly che significa «tutte le risorse».

I valori nell'elemento `Action` corrispondono alle API supportate dai servizi. Le operazioni sono precedute da `config:` a indicare che fanno riferimento alle operazioni AWS Config . Puoi utilizzare il carattere jolly `*` nell'elemento `Action`, come negli esempi seguenti:

- `"Action": ["config:*ConfigurationRecorder"]`

  Ciò consente tutte le AWS Config azioni che terminano con "ConfigurationRecorder" (`StartConfigurationRecorder`,`StopConfigurationRecorder`).
- `"Action": ["config:*"]`

  Ciò consente tutte le AWS Config azioni, ma non le azioni per altri AWS servizi.
- `"Action": ["*"]`

  Ciò consente tutte le AWS azioni. Questa autorizzazione è adatta a un utente che funge da AWS amministratore del tuo account.

La policy di sola lettura non concede autorizzazioni all'utente per operazioni come `StartConfigurationRecorder`, `StopConfigurationRecorder` e `DeleteConfigurationRecorder`. Gli utenti con questa policy non possono avviare, arrestare o cancellare la registrazione della configurazione. Per l'elenco delle AWS Config azioni, consulta l'AWS Config API Reference.

Accesso completo a AWS Config

L'esempio seguente mostra una politica che garantisce l'accesso completo a AWS Config. Concede agli utenti il permesso di eseguire tutte le AWS Config azioni. Consente inoltre agli utenti di gestire i file nei bucket Amazon S3 e gli argomenti Amazon SNS nell'account a cui è associato l'utente.

> **Important**
>
> Questa policy concede autorizzazioni ampie. Prima di concedere l'accesso completo, prendi in considerazione l'idea di iniziare con un set di autorizzazioni minimo e concedere le autorizzazioni aggiuntive quando necessario. Questa è una best practice preferibile ad iniziare con autorizzazioni che siano troppo permissive e cercare di limitarle in un secondo momento.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
                "sns:SetTopicAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
```

```
        }

    ]
}
```

Autorizzazioni supportate a livello di risorsa per le azioni dell'API Rule AWS Config

Le autorizzazioni a livello di risorsa si riferiscono alla capacità di specificare su quali risorse gli utenti possono eseguire azioni. AWS Config supporta le autorizzazioni a livello di risorsa per determinate azioni dell'API delle regole. AWS Config Ciò significa che per determinate azioni delle AWS Config regole, è possibile controllare le condizioni in base alle quali gli utenti sono autorizzati a utilizzare tali azioni. Queste condizioni possono essere azioni da eseguire o specifiche risorse che gli utenti sono autorizzati a utilizzare.

La tabella seguente descrive le azioni dell'API delle AWS Config regole che attualmente supportano le autorizzazioni a livello di risorsa. Descrive inoltre le risorse supportate e i relativi ARN per ogni azione. Quando specifichi un ARN, puoi utilizzare il carattere jolly * nei percorsi, ad esempio quando non puoi o non vuoi specificare gli ID risorsa.

> **Important**
>
> Se un'azione API della AWS Config regola non è elencata in questa tabella, significa che non supporta le autorizzazioni a livello di risorsa. Se un'azione della AWS Config regola non supporta le autorizzazioni a livello di risorsa, è possibile concedere agli utenti le autorizzazioni per utilizzare l'azione, ma è necessario specificare un* per l'elemento risorsa della dichiarazione politica.

Operazione API	Risorse
DeleteConfigRegola	Regola di configurazione arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DeleteEvaluationRisultati	Regola di configurazione arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*

Operazione API	Risorse
DescribeCompliance ByConfigRegola	Regola di configurazione arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DescribeConfigRuleEvaluatio nStato	Regola di configurazione arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
GetComplianceDetailsByConfi gRule	Regola di configurazione arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutConfigRegola	Regola di configurazione arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
StartConfigRulesEvaluation	Regola di configurazione arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutRemediationConfigurazioni	Configurazione di correzione arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediationConfigur azioni	Configurazione di correzione arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DeleteRemediationConfiguraz ione	Configurazione di correzione arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*

Operazione API	Risorse
PutRemediationEccezioni	Configurazione di correzione arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediationEccezioni	Configurazione di correzione arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DeleteRemediationEccezioni	Configurazione di correzione arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*

Se, ad esempio, si desidera consentire l'accesso in lettura e negare l'accesso in scrittura a regole specifiche a utenti specifici.

Nella prima politica, consenti alla AWS Config regola di leggere le azioni, ad esempio `DescribeConfigRuleEvaluationStatus` sulle regole specificate.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "config:StartConfigRulesEvaluation",
                    "config:DescribeComplianceByConfigRule",
                    "config:DescribeConfigRuleEvaluationStatus",
                    "config:GetComplianceDetailsByConfigRule"
                ],
                "Resource": [
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID",
```

```
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID"
                ]
            }
        ]
    }
```

Nella seconda politica, neghi alla AWS Config regola le azioni di scrittura sulla regola specifica.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
               ],
            "Resource": "arn:aws:config:region:accountID:config-rule/config-rule-ID"
           }
      ]
   }
```

Con le autorizzazioni a livello di risorsa, puoi consentire l'accesso in lettura e negare l'accesso in scrittura per eseguire azioni specifiche sulle azioni dell'API delle regole. AWS Config

Autorizzazioni a livello di risorsa supportate per l'aggregazione dei dati multi-regione multi-account

Puoi utilizzare le autorizzazioni a livello di risorsa per controllare la capacità di un utente di eseguire azioni specifiche sull'aggregazione dei dati multi-regione multi-account. Le seguenti API supportano le autorizzazioni a livello di risorsa: AWS Config `Aggregator`

- BatchGetAggregateResourceConfig
- DeleteConfigurationAggregatore
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSourcesStato
- GetAggregateComplianceDetailsByConfigRegola

- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary
- GetAggregateDiscoveredResourceConta
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources
- PutConfigurationAggregatore
- SelectAggregateResourceConfig

Ad esempio, puoi limitare l'accesso ai dati delle risorse da parte di utenti specifici creando due aggregatori `AccessibleAggregator` e `InAccessibleAggregator` e allegando una policy IAM che consente l'accesso a `AccessibleAggregator`, ma lo nega a `InAccessibleAggregator`.

Politica IAM per AccessibleAggregator

Tramite questa policy, puoi consentire l'accesso alle azioni dell'aggregatore supportate per il nome della risorsa Amazon (ARN) AWS Config specificato. In questo esempio, l' AWS Config ARN è. `arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-mocpsqhs`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
```

```
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-mocpsqhs"
        }
    ]
}
```

Politica IAM per InAccessibleAggregator

In questo criterio, neghi l'accesso alle azioni di aggregazione supportate per l' AWS Config ARN specificato. In questo esempio, l' AWS Config ARN è. `arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-pokxzldx`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

Se un utente del gruppo di sviluppatori tenta di eseguire una di queste azioni sull' AWS Config ARN specificato, quell'utente riceverà un'eccezione di accesso negato.

Verifica delle autorizzazioni di accesso degli utenti

Per mostrare gli aggregatori che hai creato, esegui il comando seguente: AWS CLI

```
aws configservice describe-configuration-aggregators
```

Quando il comando è completato correttamente, potrai vedere i dettagli di tutti gli aggregatori associati all'account. In questo esempio, sono `AccessibleAggregator` e `InAccessibleAggregator`:

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
```

```
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

> **Note**
>
> Alla voce `account-aggregation-sources` inserisci un elenco separato da virgole di ID account AWS per i quali desideri aggregare i dati. Racchiudi l'ID account tra parentesi quadre e assicurati di fare l'escape delle virgolette (ad esempio, `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`).

Collega la seguente policy IAM per negare l'accesso a `InAccessibleAggregator` o l'aggregatore a cui desideri negare l'accesso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
```

```
        }
    ]
}
```

Quindi, puoi confermare che la policy IAM funge da limitazione dell'accesso a un aggregatore specifico:

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

Il comando deve restituire un'eccezione di accesso negato:

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

AWS politiche gestite per AWS Config

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AWSConfigServiceRolePolicy

AWS Config utilizza il ruolo collegato al servizio denominato AWSServiceRoleForConfigper chiamare altri AWS servizi per conto dell'utente. Quando si utilizza il AWS Management Console per configurare AWS Config, questa reflex viene creata automaticamente AWS Config se si seleziona l'opzione per utilizzare la AWS Config reflex anziché il proprio ruolo di servizio AWS Identity and Access Management (IAM).

L'SLR AWSServiceRoleForConfig contiene la policy gestita `AWSConfigServiceRolePolicy`. Questa policy gestita contiene autorizzazioni di sola lettura e di sola scrittura per le risorse e autorizzazioni di sola lettura per AWS Config le risorse di altri servizi che le supportano. AWS Config Per ulteriori informazioni, consulta Tipi di risorsa supportati e Utilizzo dei ruoli collegati ai servizi per AWS Config.

AWSConfigServiceRolePolicyVisualizza la politica:.

AWS politica gestita: AWS_ConfigRole

Per registrare le configurazioni AWS delle risorse, sono AWS Config necessarie le autorizzazioni IAM per ottenere i dettagli di configurazione delle risorse. Se desideri creare un ruolo IAM per AWS Config, puoi utilizzare la policy gestita `AWS_ConfigRole` e collegarla al ruolo IAM.

Questa policy IAM viene aggiornata ogni volta che viene AWS Config aggiunto il supporto per un tipo di AWS risorsa. Ciò significa che AWS Config continuerà ad avere le autorizzazioni necessarie per registrare i dati di configurazione dei tipi di risorse supportati purché al ConfigRole ruolo AWS_ sia associata questa policy gestita. Per ulteriori informazioni, consulta Tipi di risorsa supportati e Autorizzazioni per il ruolo IAM assegnato a AWS Config.

Visualizza la policy: AWS_. ConfigRole

AWS politica gestita: AWSConfigUserAccess

Questa policy IAM fornisce l'accesso all'uso AWS Config, inclusa la ricerca per tag sulle risorse e la lettura di tutti i tag. Ciò non fornisce l'autorizzazione alla configurazione AWS Config, che richiede privilegi amministrativi.

Visualizza la politica: AWSConfigUserAccess.

AWS politica gestita: ConfigConformsServiceRolePolicy

Per distribuire e gestire i pacchetti di conformità, sono AWS Config necessarie le autorizzazioni IAM e alcune autorizzazioni di altri servizi. AWS Questi consentono di distribuire e gestire pacchetti di conformità con funzionalità complete e vengono aggiornati ogni volta che vengono aggiunte nuove funzionalità per i pacchetti di conformità. AWS Config Per ulteriori informazioni sui pacchetti di conformità, consulta Pacchetti di conformità.

Visualizza la politica: Politica. ConfigConforms ServiceRole

AWS politica gestita: AWSConfigRulesExecutionRole

Per implementare regole Lambda AWS personalizzate AWS Config , sono necessarie le autorizzazioni IAM e alcune autorizzazioni di altri servizi. AWS Questi consentono alle AWS Lambda funzioni di accedere all' AWS Config API e agli snapshot di configurazione che vengono AWS Config distribuiti periodicamente ad Amazon S3. Questo accesso è richiesto dalle funzioni che valutano le modifiche alla configurazione per le regole Lambda AWS personalizzate e viene aggiornato ogni volta che vengono AWS Config aggiunte nuove funzionalità. Per ulteriori informazioni sulle regole Lambda AWS personalizzate, vedere Creazione di regole AWS Config Lambda personalizzate e componenti di una regola. AWS Config Per ulteriori informazioni sugli snapshot di configurazione, consulta Concetti | Snapshot di configurazione. Per ulteriori informazioni sulla distribuzione degli snapshot di configurazione, consulta Gestione del canale di distribuzione.

Visualizza la politica:. AWSConfigRulesExecutionRole

AWS politica gestita: AWSConfigMultiAccountSetupPolicy

Per distribuire, aggiornare ed eliminare centralmente AWS Config regole e pacchetti di conformità tra gli account dei membri di un'organizzazione in AWS Organizations, sono AWS Config necessarie le autorizzazioni IAM e determinate autorizzazioni di altri servizi. AWS Questa policy gestita viene aggiornata ogni volta che vengono AWS Config aggiunte nuove funzionalità per la configurazione di più account. Per ulteriori informazioni, consulta Gestione delle AWS Config regole per tutti gli account dell'organizzazione e Gestione dei pacchetti di conformità per tutti gli account dell'organizzazione.

Visualizza la politica:. AWSConfigMultiAccountSetupPolicy

AWS politica gestita: AWSConfigRoleForOrganizations

Per consentire di AWS Config chiamare AWS Organizations API di sola lettura, AWS Config richiede le autorizzazioni IAM e alcune autorizzazioni di altri servizi. AWS Questa policy gestita viene

aggiornata ogni volta che vengono AWS Config aggiunte nuove funzionalità per la configurazione di più account. Per ulteriori informazioni, consulta Gestione delle AWS Config regole per tutti gli account dell'organizzazione e Gestione dei pacchetti di conformità per tutti gli account dell'organizzazione.

Visualizza la politica:. AWSConfigRoleForOrganizations

AWS politica gestita: AWSConfigRemediationServiceRolePolicy

AWS Config Per consentire la riparazione `NON_COMPLIANT` delle risorse per tuo conto, AWS Config richiede le autorizzazioni IAM e alcune autorizzazioni di altri servizi. AWS Questa policy gestita viene aggiornata ogni volta che vengono AWS Config aggiunte nuove funzionalità per la correzione. Per ulteriori informazioni sulla riparazione, vedere Riparazione di risorse non conformi con regole. AWS Config Per ulteriori informazioni sulle condizioni che determinano i possibili risultati della AWS Config valutazione, vedere Concetti | Regole. AWS Config

Visualizza la politica: AWSConfigRemediationServiceRolePolicy.

AWS Config aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS Config da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei AWS Config documenti.

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di elasticfilesystem:DescribeTags," "redshift:DescribeTags", and "ssm-sap:ListTagsForResource"	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Elastic File System (Amazon EFS), Amazon AWS Systems Manager per SAP Redshift e.	17 giugno 2024
AWSConfigServiceRolePolicy: aggiunta di elasticfilesystem: DescribeTags," "redshift:DescribeTags", and "ssm-sap:ListTagsForResource"	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Elastic File System (Amazon EFS), Amazon AWS Systems Manager per SAP Redshift e.	17 giugno 2024

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments,	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Service for Prometheus, Amazon, Amazon CloudWatch Cognito, Amazon, Amazon FSx, AWS Identity and Access Management (IAM) ElastiCache,, Amazon AWS RAM Redshift Serverless AWS Glue, Amazon e Amazon Simple Notification Service (Amazon SNS). AWS Lambda SageMaker	22 febbraio 2024

Modifica	Descrizione	Data
" and "sns:GetSMSSandboxAccountStatus"		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments,	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Service for Prometheus, Amazon, Amazon CloudWatch Cognito, Amazon, Amazon FSx, AWS Identity and Access Management (IAM) ElastiCache,, Amazon AWS RAM Redshift Serverless AWS Glue, Amazon e Amazon Simple Notification Service (Amazon SNS). AWS Lambda SageMaker	22 febbraio 2024

Modifica	Descrizione	Data
" and "sns:GetSMSSandboxAccountStatus"		
AWSConfigUserAccess— AWS Config inizia a tenere traccia delle modifiche apportate a questa politica AWS gestita	Questa politica fornisce l'accesso all'uso AWS Config, inclusa la ricerca per tag sulle risorse e la lettura di tutti i tag. Ciò non fornisce l'autorizzazione alla configurazione AWS Config, che richiede privilegi amministrativi.	22 febbraio 2024
AWS_ConfigRole: aggiunta di "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Service for Prometheus AWS AppConfig, () AWS Database Migration Service , AWS DMS(AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Logs CloudWatch e Amazon Simple Storage Service (Amazon S3). AWS Organizations	5 dicembre 2023

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Service for Prometheus AWS AppConfig, () AWS Database Migration Service , AWS DMS(AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Logs CloudWatch e Amazon Simple Storage Service (Amazon S3). AWS Organizations	5 dicembre 2023

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationA	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Cognito, Amazon Connect, Amazon EMR,, AWS Ground Station, Amazon MemoryDB for Redis AWS Mainframe Modernization, Amazon AWS Organizations, Amazon QuickSight Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53 e. AWS Service Catalog AWS Transfer Family	17 novembre 2023

Modifica	Descrizione	Data
ssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrLocations,"		

Modifica	Descrizione	Data
"serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWS_ConfigRole: aggiunta di "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	Questa policy ora aggiunge identificatori di sicurezza (SID) per `AWSConfigServiceRolePolicyStatementID`, `AWSConfigSLRLogStatementID`, `AWSConfigSLRLogEventStatementID` e `AWSConfigSLRApiGatewayStatementID`.	17 novembre 2023

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationA	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Cognito, Amazon Connect, Amazon EMR,, AWS Ground Station, Amazon MemoryDB for Redis AWS Mainframe Modernization, Amazon AWS Organizations, Amazon QuickSight Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53 e. AWS Service Catalog AWS Transfer Family	17 novembre 2023

Modifica	Descrizione	Data
ssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrLocations,"		

Modifica	Descrizione	Data
"serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWSConfigServiceRolePolicy: aggiunta di "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	Questa policy ora aggiunge identificatori di sicurezza (SID) per `AWSConfigServiceRolePolicyStatementID`, `AWSConfigSLRLogStatementID`, `AWSConfigSLRLogEventStatementID` e `AWSConfigSLRApiGatewayStatementID`.	17 novembre 2023

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListTags,	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Connect AWS Private CA AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Evidently, Amazon Managed Grafana, Amazon, Amazon Inspector,, Amazon Managed Streaming for Apache Kafka (Amazon MSK) GuardDuty, e Amazon AWS IoT Managed AWS IoT TwinMaker Streaming for Apache Kafka (Amazon MSK) e Amazon. AWS Lambda AWS Network Manager AWS Organizations SageMaker	4 ottobre 2023

Modifica	Descrizione	Data
" "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListTags,	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Connect AWS Private CA AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Evidently, Amazon Managed Grafana, Amazon, Amazon Inspector,, Amazon Managed Streaming for Apache Kafka (Amazon MSK) GuardDuty, e Amazon AWS IoT Managed AWS IoT TwinMaker Streaming for Apache Kafka (Amazon MSK) e Amazon. AWS Lambda AWS Network Manager AWS Organizations SageMaker	4 ottobre 2023

Modifica	Descrizione	Data
" "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		
AWSConfigServiceRolePolicy— Rimuovi "ssm:GetParameter"	Questa politica ora rimuove le autorizzazioni per AWS Systems Manager (Systems Manager).	6 settembre 2023

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di "appmesh:DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSecrets",	Questa politica ora supporta autorizzazioni aggiuntive per AWS App Mesh, Amazon Connect, Amazon AWS CloudFormation CloudFront AWS CodeArtifact, AWS Identity and Access Management (IAM) AWS CodeBuild, Amazon Inspector AWS Glue, GuardDuty,,, Amazon Managed Streaming for Apache Kafka AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon AWS Network Manager Esploratore di risorse AWS Macie,,,, , Amazon Route 53, AWS Elemental MediaConnect Amazon Simple Storage Service (AWS Organizations Amazon S3) e Amazon Simple Storage Service (Amazon S3) e Amazon Simple Servizio di notifica (Amazon SNS).	28 luglio 2023

Modifica	Descrizione	Data
"macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy"		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di "appmesh: DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSecrets", "m	Questa politica ora supporta autorizzazioni aggiuntive per Amazon AppStream 2.0 AWS App Mesh, Amazon,,, AWS CloudFormation, Amazon Connect CloudFront AWS CodeArtifact AWS CodeBuild, AWS Identity and Access Management (IAM) AWS Glue, Amazon Inspector GuardDuty,,,, Amazon Managed Streaming for Apache Kafka AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon AWS Network Manager Esploratore di risorse AWS Macie,,,, , Amazon Route 53, AWS Elemental MediaConnect AWS Organizations Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS) e Amazon EC2 Systems Manager (SSM).	28 luglio 2023

Modifica	Descrizione	Data
acie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource"		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", “dynamodb:DescribeTableReplicaAutoScaling" "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Connect AWS Amplify, Amazon Managed Service for Prometheus AWS App Mesh, Amazon AWS Batch Athena,,,, Amazon, Amazon DynamoDB AWS CloudFormation AWS CloudTrail AWS CodeArtifact, Amazon Elastic Compute Cloud (Amazon CodeGuru EC2) Elastic Compute CloudWatch EC2) AWS Directory Service, Amazon Evidently, Amazon Forecast, , (AWS Identity and Access Management IAM), AWS Organizations Amazon Managed Streaming per Apache Kafka AWS Ground Station(Amazon MSK), Amazon Lightsail, Amazon Logs,, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon AWS IoT Greengrass CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor VPC), Amazon Personalize, Amazon AWS Migration Hub Refactor Spaces, QuickSight Amazon Simple Storage Service (Amazon S3),	13 giugno 2023

Modifica	Descrizione	Data
tasetGroup", "forecast :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases" "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "org	Amazon,. SageMaker AWS Transfer Family	

Modifica	Descrizione	Data
anizations:ListAccountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Connect AWS Amplify, Amazon Managed Service for Prometheus AWS App Mesh, Amazon AWS Batch Athena,,,, Amazon, Amazon DynamoDB AWS CloudFormation AWS CloudTrail AWS CodeArtifact, Amazon Elastic Compute Cloud (Amazon CodeGuru EC2) Elastic Compute CloudWatch EC2) AWS Directory Service, Amazon Evidently, Amazon Forecast, , (AWS Identity and Access Management IAM), AWS Organizations Amazon Managed Streaming per Apache Kafka AWS Ground Station(Amazon MSK), Amazon Lightsail, Amazon Logs,, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon AWS IoT Greengrass CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor VPC), Amazon Personalize, Amazon AWS Migration Hub Refactor Spaces, QuickSight Amazon Simple Storage Service (Amazon S3),	13 giugno 2023

Modifica	Descrizione	Data
tasetGroup", "forecast :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts",	Amazon,. SageMaker AWS Transfer Family	

Modifica	Descrizione	Data
"organizations:ListAccountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfigurat	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Workflows for AWS Amplify,, AWS App Runner Amazon AWS App Mesh CloudFront, AWS CodeArtifact Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon, Amazon AWS Migration Hub Pinpoint, AWS Resilience AWS Transfer Family Hub SageMaker, Amazon, Directory Service e. CloudWatch AWS AWS WAF	13 aprile 2023

Modifica	Descrizione	Data
ion, macie2:GetClassificationExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, ec2:GetInstanceTypesFromInstanceRequirement, ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfiguration, macie2:GetClassificati	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Workflows for AWS Amplify,, AWS App Runner Amazon AWS App Mesh CloudFront, AWS CodeArtifact Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon, Amazon AWS Migration Hub Pinpoint, AWS Resilience AWS Transfer Family Hub SageMaker, Amazon, Directory Service e. CloudWatch AWS AWS WAF	13 aprile 2023

Modifica	Descrizione	Data
onExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudfront:GetResponseHeadersPolicy, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAML	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Workflows for Amazon AppFlow, AWS App Runner Amazon AppStream 2.0, Amazon, CloudWatch,,, CloudFront Amazon CloudWatch Evidently AWS CodeArtifact AWS CodeCommit, AWS Device Farm Amazon Forecast, AWS Identity and Access Management (IAM) AWS Ground Station, Amazon MemoryDB for Redis, AWS IoT Amazon Pinpoint, Amazon AWS Network Manager Relational Database AWS Panorama Service (Amazon RDS), Amazon Redshift e Amazon. SageMaker	30 marzo 2023

Modifica	Descrizione	Data
Provider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundsta	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Workflows for Amazon AppFlow, Amazon AppStream 2.0, AWS App Runner Amazon,,, CloudWatch AWS CodeArtifact, AWS CloudFormation CloudFront Amazon Elastic Compute Cloud (AWS Device Farm Amazon EC2) AWS CodeCommit, Amazon Evidently, Amazon Forecast, AWS Identity and Access Management (IAM) CloudWatch , Amazon MemoryDB for Redis AWS Ground Station, Amazon Pinpoint, AWS IoT Amazon AWS Network Manager Relational Database Service Database Service (Amazon RDS), Amazon Redshift e AWS Panorama Amazon. SageMaker	30 marzo 2023

Modifica	Descrizione	Data
tion:GetConfig, groundst ation:ListConfigs, groundst ation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate, i am:ListAccessKeys, iam:List Groups, iam:ListInstancePro files, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAM LProviders, iot:DescribeFle etMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobile targeting:GetApp, mobiletar geting:GetCampaigns, networ kmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, p anorama:ListNodes, rds:Desc ribeDBProxyEndpoints, redsh ift:DescribeScheduledActions, sagemaker:DescribeAppIma geConfig, sagemaker:Describ eImage, sagemaker:DescribeI mageVersion, sagem aker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Modifica	Descrizione	Data
AWSConfigRulesExecutionRole— inizia a tenere traccia delle modifiche per questa AWS Config policy gestita AWS	Questa policy consente alle AWS Lambda funzioni di accedere all' AWS Config API e agli snapshot di configurazione che vengono AWS Config distribuiti periodicamente ad Amazon S3. Questo accesso è richiesto dalle funzioni che valutano le modifiche alla configurazione per le regole Lambda AWS personalizzate.	7 marzo 2023
AWSConfigRoleForOrganizations— AWS Config inizia a tenere traccia delle modifiche per questa politica AWS gestita	Questa policy consente di AWS Config chiamare API di sola lettura AWS Organizations .	7 marzo 2023
AWSConfigRemediationServiceRolePolicy— AWS Config inizia a tenere traccia delle modifiche per questa policy gestita AWS	Questa politica consente di AWS Config ripristinare le `NON_COMPLIANT` risorse per conto dell'utente.	7 marzo 2023
AWSConfigServiceRolePolicy: aggiunta di auditmanager:GetAccountStatus	Questa policy ora concede l'autorizzazione per restituire lo stato di registrazione di un account in AWS Audit Manager.	3 marzo 2023

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di auditmanager:GetAccountStatus	Questa policy ora concede l'autorizzazione per restituire lo stato di registrazione di un account in AWS Audit Manager.	3 marzo 2023
AWSConfigMultiAccountSetupPolicy— AWS Config inizia a tenere traccia delle modifiche apportate a questa politica AWS gestita	Questa politica consente di AWS Config chiamare AWS i servizi e distribuire AWS Config risorse all'interno di un'organizzazione con AWS Organizations.	27 febbraio 2023

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefarm:L	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Workflows for Apache Airflow, AWS IoT Amazon 2.0 AppStream , Amazon CodeGuru Reviewer, Amazon Kinesis AWS HealthLake Video Streams, Amazon Route 53 Application Recovery Controller, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint (IAM) AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon e Amazon Logs. AWS Identity and Access Management GuardDuty CloudWatch	1 febbraio 2023

Modifica	Descrizione	Data
istTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di airflow:ListTagsForResource , iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Workflows for Apache Airflow, AWS IoT Amazon 2.0 AppStream , Amazon CodeGuru Reviewer, Amazon Kinesis AWS HealthLake Video Streams, Amazon Route 53 Application Recovery Controller, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint (IAM) AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon e Amazon Logs. AWS Identity and Access Management GuardDuty CloudWatch	1 febbraio 2023

Modifica	Descrizione	Data
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy: aggiornamento di config:DescribeConfigRules	Come best practice di sicurezza, questa policy ora rimuove l'autorizzazione ampia a livello di risorsa per `config:DescribeConfigRules` .	12 gennaio 2023

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsFor	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm, Amazon Elastic Compute Cloud AWS Database Migration Service (Amazon EC2 AWS DMS) AWS Directory Service, Amazon Lightsail, Amazon, Amazon, Amazon AWS Glue AWS IoT, Amazon Route 53 Application Recovery Controller AWS Elemental MediaPackage AWS Network Manager, Amazon Simple Storage Service (QuickSight AWS Resource Access Manager Amazon S3) e Amazon Amazon Timestream.	15 dicembre 2022

Modifica	Descrizione	Data
Resource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsFor	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm, Amazon Elastic Compute Cloud AWS Database Migration Service (Amazon EC2 AWS DMS) AWS Directory Service, Amazon Lightsail, Amazon, Amazon, Amazon AWS Glue AWS IoT, Amazon Route 53 Application Recovery Controller AWS Elemental MediaPackage AWS Network Manager, Amazon Simple Storage Service (QuickSight AWS Resource Access Manager Amazon S3) e Amazon Amazon Timestream.	15 dicembre 2022

Modifica	Descrizione	Data
Resource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di cloudformation:ListStackResources and cloudformation:ListStacks	Questa politica ora concede l'autorizzazione a restituire le descrizioni di tutte le risorse di uno AWS CloudFormation stack specificato e a restituire le informazioni di riepilogo per gli stack il cui stato corrisponde a quello specificatoStackStatusFilter.	7 novembre 2022
AWS_ConfigRole: aggiunta di cloudformation:ListStackResources and cloudformation:ListStacks	Questa politica ora concede l'autorizzazione a restituire le descrizioni di tutte le risorse di uno stack specificato e a restituire le informazioni di riepilogo per gli AWS CloudFormation stack il cui stato corrisponde a quello specificato. StackStatusFilter	7 novembre 2022

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVersi	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Workflows for Apache Airflow AWS Certificate Manager, Amazon Keyspaces, Amazon, Amazon Connect, AWS Amplify Amazon Elastic Compute Cloud (AWS AppConfig Amazon EC2), CloudWatch Amazon Elastic Kubernetes Service (Amazon EKS) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon Fraud Detector, Amazon Fraud Detector EventBridge, Amazon Fraud Detector FSx, AWS Fault Injection Service Amazon, Amazon Location Service, Amazon Lex, Amazon Lightsail, GameLift Amazon Pinpoint,,, Amazon AWS IoT, Amazon, Amazon Relational Database Service (Amazon RDS), AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Amazon AWS RoboMaker Rekognition AWS Resource Groups,,, Amazon Route 53, Amazon Simple Storage AWS	19 ottobre 2022

Modifica	Descrizione	Data
ons, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, iotsite	Cloud Map Service (Amazon S3) e. AWS Security Token Service	

Modifica	Descrizione	Data
wise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanceDetails, panorama:DescribePackage		

Modifica	Descrizione	Data
, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVersions, databrew:ListRulesets,	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Workflows for Apache Airflow AWS Certificate Manager, Amazon Keyspaces, Amazon, Amazon Connect, AWS Amplify Amazon Elastic Compute Cloud (AWS AppConfig Amazon EC2), CloudWatch Amazon Elastic Kubernetes Service (Amazon EKS) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon Fraud Detector, Amazon Fraud Detector EventBridge, Amazon Fraud Detector FSx, AWS Fault Injection Service Amazon, Amazon Location Service, Amazon Lex, Amazon Lightsail, GameLift Amazon Pinpoint,,, Amazon AWS IoT, Amazon, Amazon Relational Database Service (Amazon RDS), AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Amazon AWS RoboMaker Rekognition AWS Resource Groups,,, Amazon Route 53, Amazon Simple Storage AWS	19 ottobre 2022

Modifica	Descrizione	Data
databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, iotsitewise:ListAssetModels, iotsit	Cloud Map Service (Amazon S3) e. AWS Security Token Service	

Modifica	Descrizione	Data
ewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanceDetails, panorama:DescribePackage, panorama:Describe		

Modifica	Descrizione	Data
PackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di Glue::GetTable	Questa politica ora concede l'autorizzazione a recuperare la definizione della AWS Glue tabella in un catalogo dati per una tabella specificata.	14 settembre 2022
AWS_ConfigRole: aggiunta di Glue::GetTable	Questa politica ora concede l'autorizzazione a recuperare la definizione della AWS Glue tabella in un catalogo dati per una tabella specificata.	14 settembre 2022

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirr	Questa policy ora supporta autorizzazioni aggiuntive per Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon Guru, DevOps Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon Amazon FinSpace Schemas,, Amazon Fraud Detector, Amazon, Amazon EventBridge Interactive Video Service (EventBridge Amazon IVS), Amazon Managed Service per Apache Flink GameLift, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon StudioAmazon Nimble Pinpoint QuickSight, Amazon, Amazon, Controller di Amazon Route 53 Resolver ripristino delle applicazioni Amazon Route 53, Amazon	7 settembre 2022

Modifica	Descrizione	Data
orFilters, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, game	Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup Budget AWS AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker,,,, e. AWS Lake Formation AWS License Manager AWS Resilience Hub AWS Signer AWS Transfer Family	

Modifica	Descrizione	Data
lift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:Desc		

Modifica	Descrizione	Data
ribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, ioteventsDescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, ioteventsListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets		

Modifica	Descrizione	Data
, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:Ge		

Modifica	Descrizione	Data
tInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletargeting:		

Modifica	Descrizione	Data
ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies,		

Modifica	Descrizione	Data
route53-recovery-readiness: GetCell, route53-recovery-re adiness:GetReadinessCheck, route53-recovery-readiness:G etRecoveryGroup, route53- recovery-readiness:Ge tResourceSet, route53- recovery-readiness:ListC ells, route53-recovery-readi ness:ListReadinessChecks, route53-recovery-readiness:Li stRecoveryGroups, route53- recovery-readiness:ListResour ceSets, route53resolver:GetF irewallDomainList, route53re solver:GetFirewallRuleGroup , route53resolver:GetFirewal lRuleGroupAssociation, route53resolver:GetReso lverQueryLogConfig, route53r esolver:ListFirewallDomainL ists, route53resolver:ListFi rewallDomains, route53resolv er:ListFirewallRuleGroupAss ociations, route53resolver:L istFirewallRuleGroups, route53resolver:ListFir ewallRules, route53resolver: ListResolverQueryLogConfigs , rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, ru m:ListTagsForResource, s3- outposts:GetAccessPoint, s3-outposts:GetAccessPo		

Modifica	Descrizione	Data
intPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUs		

Modifica	Descrizione	Data
er, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTargets,	Questa policy ora supporta autorizzazioni aggiuntive per Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon Guru, DevOps Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon Amazon FinSpace Schemas,, Amazon Fraud Detector, Amazon, Amazon EventBridge Interactive Video Service (EventBridge Amazon IVS), Amazon Managed Service per Apache Flink GameLift, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon StudioAmazon Nimble Pinpoint QuickSight, Amazon, Amazon, Controller di Amazon Route 53 Resolver ripristino delle applicazioni Amazon Route 53, Amazon	7 settembre 2022

Modifica	Descrizione	Data
ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocationAttributes, gamel	Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup Budget AWS AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker,,,, e AWS Lake Formation AWS License Manager AWS Resilience Hub AWS Signer AWS Transfer Family	

Modifica	Descrizione	Data
ift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination		

Modifica	Descrizione	Data
, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwi		

Modifica	Descrizione	Data
nmaker:ListEntities, iottwin maker:ListScenes, iottwinmak er:ListTagsForResource, iott winmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfigura tion, ivs:GetStreamKey, ivs:ListChannels, ivs:Li stPlaybackKeyPairs, ivs:List RecordingConfigurations, ivs:ListStreamKeys, iv s:ListTagsForResource, kines isanalytics:ListApplications, lakeformation:DescribeRes ource, lakeformation:GetData LakeSettings, lakeformation: ListPermissions, lakeformati on:ListResources, lex:Descri beBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:List BotLocales, lex:ListBots, lex :ListTagsForResource, licens e-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLice nses, license-manager:ListRe ceivedGrants, lightsail:GetA larms, lightsail:GetBuckets, lightsail:GetCertificates, l ightsail:GetDisk, lightsail: GetDisks, lightsail:GetInsta nce, lightsail:GetInstances, lightsail:GetKeyPair, lights		

Modifica	Descrizione	Data
ail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile,		

Modifica	Descrizione	Data
nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetRead		

Modifica	Descrizione	Data
inessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPointPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetL		

Modifica	Descrizione	Data
ifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:		

Modifica	Descrizione	Data
ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject,	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Workflows for Apache Airflow, AWS IoT Amazon 2.0 AppStream , Amazon CodeGuru Reviewer, Amazon Kinesis AWS HealthLake Video Streams, Amazon Route 53 Application Recovery Controller, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint (IAM) AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon e Amazon Logs. AWS Identity and Access Management GuardDuty CloudWatch	1 febbraio 2023

Modifica	Descrizione	Data
devicefarm:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Workflows for Apache Airflow, AWS IoT Amazon 2.0 AppStream , Amazon CodeGuru Reviewer, Amazon Kinesis AWS HealthLake Video Streams, Amazon Route 53 Application Recovery Controller, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint (IAM) AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon e Amazon Logs. AWS Identity and Access Management GuardDuty CloudWatch	1 febbraio 2023

Modifica	Descrizione	Data
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy: aggiornamento di config:DescribeConfigRules	Come best practice di sicurezza, questa policy ora rimuove l'autorizzazione ampia a livello di risorsa per `config:DescribeConfigRules` .	12 gennaio 2023

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm, Amazon Elastic Compute Cloud AWS Database Migration Service (Amazon EC2 AWS DMS) AWS Directory Service, Amazon Lightsail, Amazon, Amazon, Amazon AWS Glue AWS IoT, Amazon Route 53 Application Recovery Controller AWS Elemental MediaPackage AWS Network Manager, Amazon Simple Storage Service (QuickSight AWS Resource Access Manager Amazon S3) e Amazon Amazon Timestream.	15 dicembre 2022

Modifica	Descrizione	Data
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm, Amazon Elastic Compute Cloud AWS Database Migration Service (Amazon EC2 AWS DMS) AWS Directory Service, Amazon Lightsail, Amazon, Amazon, Amazon AWS Glue AWS IoT, Amazon Route 53 Application Recovery Controller AWS Elemental MediaPackage AWS Network Manager, Amazon Simple Storage Service (QuickSight AWS Resource Access Manager Amazon S3) e Amazon Amazon Timestream.	15 dicembre 2022

Modifica	Descrizione	Data
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di cloudformation:ListStackResources and cloudformation:ListStacks	Questa politica ora concede l'autorizzazione a restituire le descrizioni di tutte le risorse di uno AWS CloudFormation stack specificato e a restituire le informazioni di riepilogo per gli stack il cui stato corrisponde a quello specificatoStackStatusFilter.	7 novembre 2022
AWS_ConfigRole: aggiunta di cloudformation:ListStackResources and cloudformation:ListStacks	Questa politica ora concede l'autorizzazione a restituire le descrizioni di tutte le risorse di uno stack specificato e a restituire le informazioni di riepilogo per gli AWS CloudFormation stack il cui stato corrisponde a quello specificato. StackStatusFilter	7 novembre 2022

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Workflows for Apache Airflow AWS Certificate Manager, Amazon Keyspaces, Amazon, Amazon Connect, AWS Amplify Amazon Elastic Compute Cloud (AWS AppConfig Amazon EC2), CloudWatch Amazon Elastic Kubernetes Service (Amazon EKS) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon Fraud Detector, Amazon Fraud Detector EventBridge, Amazon Fraud Detector FSx, AWS Fault Injection Service Amazon, Amazon Location Service, Amazon Lex, Amazon Lightsail, GameLift Amazon Pinpoint,,, Amazon AWS IoT, Amazon, Amazon Relational Database Service (Amazon RDS), AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Amazon AWS RoboMaker Rekognition AWS Resource Groups,,, Amazon Route 53, Amazon Simple Storage AWS	19 ottobre 2022

Modifica	Descrizione	Data
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi	Cloud Map Service (Amazon S3) e. AWS Security Token Service	

Modifica	Descrizione	Data
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Modifica	Descrizione	Data
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Managed Workflows for Apache Airflow AWS Certificate Manager, Amazon Keyspaces, Amazon, Amazon Connect, AWS Amplify Amazon Elastic Compute Cloud (AWS AppConfig Amazon EC2), CloudWatch Amazon Elastic Kubernetes Service (Amazon EKS) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon Fraud Detector, Amazon Fraud Detector EventBridge, Amazon Fraud Detector FSx, AWS Fault Injection Service Amazon, Amazon Location Service, Amazon Lex, Amazon Lightsail, GameLift Amazon Pinpoint,,, Amazon AWS IoT, Amazon, Amazon Relational Database Service (Amazon RDS), AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Amazon AWS RoboMaker Rekognition AWS Resource Groups,,, Amazon Route 53, Amazon Simple Storage AWS	19 ottobre 2022

Modifica	Descrizione	Data
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi	Cloud Map Service (Amazon S3) e. AWS Security Token Service	

Modifica	Descrizione	Data
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Modifica	Descrizione	Data
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di Glue::GetTable	Questa politica ora concede l'autorizzazione a recuperare la definizione della AWS Glue tabella in un catalogo dati per una tabella specificata.	14 settembre 2022
AWS_ConfigRole: aggiunta di Glue::GetTable	Questa politica ora concede l'autorizzazione a recuperare la definizione della AWS Glue tabella in un catalogo dati per una tabella specificata.	14 settembre 2022

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	Questa policy ora supporta autorizzazioni aggiuntive per Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon Guru, DevOps Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon Amazon FinSpace Schemas,, Amazon Fraud Detector, Amazon, Amazon EventBridge Interactive Video Service (EventBridge Amazon IVS), Amazon Managed Service per Apache Flink GameLift, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon StudioAmazon Nimble Pinpoint QuickSight, Amazon, Amazon, Controller di Amazon Route 53 Resolver ripristino delle applicazioni Amazon Route 53, Amazon	7 settembre 2022

Modifica	Descrizione	Data
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream AWS AppSync,,,,,,,,,,,, AWS AppConfig AWS Auto Scaling AWS Backup Budget AWS AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation,,, e. AWS License Manager AWS Resilience Hub AWS Signer AWS Transfer Family	

Modifica	Descrizione	Data
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

Modifica	Descrizione	Data
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

Modifica	Descrizione	Data
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

Modifica	Descrizione	Data
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

Modifica	Descrizione	Data
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

Modifica	Descrizione	Data
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

Modifica	Descrizione	Data
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

Modifica	Descrizione	Data
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	Questa policy ora supporta autorizzazioni aggiuntive per Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon Guru, DevOps Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon Amazon FinSpace Schemas,, Amazon Fraud Detector, Amazon, Amazon EventBridge Interactive Video Service (EventBridge Amazon IVS), Amazon Managed Service per Apache Flink GameLift, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon StudioAmazon Nimble Pinpoint QuickSight, Amazon, Amazon, Controller di Amazon Route 53 Resolver ripristino delle applicazioni Amazon Route 53, Amazon	7 settembre 2022

Modifica	Descrizione	Data
ts, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat	Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream AWS AppSync,,,,,,,,,,,,, AWS AppConfig AWS Auto Scaling AWS Backup Budget AWS AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation,,, e AWS License Manager AWS Resilience Hub AWS Signer AWS Transfer Family	

Modifica	Descrizione	Data
ionAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

Modifica	Descrizione	Data
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

Modifica	Descrizione	Data
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

Modifica	Descrizione	Data
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

Modifica	Descrizione	Data
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

Modifica	Descrizione	Data
olicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

Modifica	Descrizione	Data
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

Modifica	Descrizione	Data
ansfer:DescribeUser, transfer: DescribeWorkflow, transfer: ListServers, transfer:ListUsers , transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		
AWSConfigServiceRolePolicy: aggiunta di datasync:ListAgent s, datasync:ListLocations, datasync:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists	Questa politica ora consente di restituire un elenco di AWS DataSync agenti, posizioni di DataSync origine e destinazi one e DataSync attività in un Account AWS file, elencare informazioni di riepilogo sui namespace e AWS Cloud Map i servizi associati a uno o più namespace specificati in un ed elencare tutte le liste di contatti di Amazon Simple Email Service (Amazon SES) Simple Email Service (Amazon SES) disponibili in. Account AWS Account AWS	22 agosto 2022

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di datasync:ListAgents, datasync:ListLocations, dat async:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists	Questa politica ora consente di restituire un elenco di AWS DataSync agenti, posizioni di DataSync origine e destinazi one e DataSync attività in un Account AWS file, elencare informazioni di riepilogo sui namespace e AWS Cloud Map i servizi associati a uno o più namespace specificati in un ed elencare tutte le liste di contatti di Amazon Simple Email Service (Amazon SES) Simple Email Service (Amazon SES) disponibili in. Account AWS Account AWS	22 agosto 2022
ConfigConformsServ iceRolePolicy: aggiunta di cloudwatch:PutMetricData	Questa politica ora concede l'autorizzazione a pubblicare punti dati metrici su Amazon. CloudWatch	25 luglio 2022

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Elastic Container Service (Amazon ECS), Amazon, Amazon, Amazon FSx, ElastiCache EventBridge Amazon Managed Service per Apache Flink, Amazon Location Service, Amazon Managed Streaming per Apache Kafka, Amazon, Amazon Rekognition e Amazon Simple Storage Service (Amazon S3) QuickSight, Amazon Simple Email Service (Amazon SES) AWS RoboMaker,,,,,,,, (IAM Identity Center), EC2 Image Builder ed Elastic AWS AppSync Load AWS Billing Conductor Balancing. AWS Amplify AWS AppConfig AWS DataSync AWS Firewall Manager AWS Glue AWS IAM Identity Center	15 luglio 2022

Modifica	Descrizione	Data
nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVers		

Modifica	Descrizione	Data
ions, imagebuilder: ListComponents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

Modifica	Descrizione	Data
sso:GetInlinePolicyForPermissionSet		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De	Questa policy ora supporta autorizzazioni aggiuntive per Amazon Elastic Container Service (Amazon ECS), Amazon, Amazon, Amazon FSx, ElastiCache EventBridge Amazon Managed Service per Apache Flink, Amazon Location Service, Amazon Managed Streaming per Apache Kafka, Amazon, Amazon Rekognition e Amazon Simple Storage Service (Amazon S3) QuickSight, Amazon Simple Email Service (Amazon SES) AWS RoboMaker,,,,,,,, (IAM Identity Center), EC2 Image Builder ed Elastic AWS AppSync Load AWS Billing Conductor Balancing. AWS Amplify AWS AppConfig AWS DataSync AWS Firewall Manager AWS Glue AWS IAM Identity Center	15 luglio 2022

Modifica	Descrizione	Data
scribeLocationS3, datasync: DescribeLocationSmb, datasy nc:DescribeTask, datasync: ListTagsForResource, ecr:De scribePullThroughCacheRules , ecr:DescribeRegistry, ecr:G etRegistryPolicy, elasticac he:DescribeCacheParameters, elasticloadbalancing:Descr ibeListenerCertificates, el asticloadbalancing:Describe TargetGroupAttributes, elas ticloadbalancing:DescribeTa rgetGroups, elasticloadbala ncing:DescribeTargetHealth, events:DescribeApiDestinat ion, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListP olicies, fms:ListTagsForRes ource, fsx:DescribeVolumes, geo:DescribeGeofenceColl ection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator , geo:DescribeTracker, geo:ListTrackerConsumers, g lue:BatchGetJobs, glue:Batc hGetWorkflows, glue:GetC rawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuil der: GetComponent, imagebuil der: ListComponentBuildVers ions, imagebuilder: ListCompo		

Modifica	Descrizione	Data
nents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

Modifica	Descrizione	Data
sso:GetInlinePolicyForPermissionSet		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAtt	Questa policy ora concede l'autorizzazione a ottenere un catalogo dati Amazon Athena specifico, elencare i cataloghi di dati Athena in Account AWS un ed elencare i tag associati a un gruppo di lavoro o a una risorsa del catalogo dati Athena; ottenere un elenco di grafici comportamentali di Amazon Detective e tag di elenco per un grafico di comportamento di Detective; ottenere un elenco di metadati di risorse per un determinato elenco di nomi di endpoint di sviluppo, ottenere informazioni su un endpoint AWS Glue di sviluppo specificato, ottieni tutti gli endpoint di sviluppo in un file, recupera una sicurezza AWS Glue specificata AWS Glue Account AWS AWS Glue configurazione, ottieni tutte le configurazioni di AWS Glue sicurezza, ottieni un elenco di tag associati a una AWS Glue risorsa, ottieni informazioni su un AWS Glue gruppo di lavoro con il nome specificato, recupera i nomi di tutte le risorse AWS Glue crawler in un AWS account, ottieni i nomi di tutte le AWS Glue	31 maggio 2022

Modifica	Descrizione	Data
ributeConfiguration, sso:DescribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	`DevEndpoint` risorse in un Account AWS, elenca i nomi di tutte le risorse di AWS Glue lavoro in un Account AWS, ottieni dettagli sugli account AWS Glue membro, elenca i nomi dei AWS Glue flussi di lavoro creati in un account ed elenca i AWS Glue gruppi di lavoro disponibili per un account; recuperare e dettagli su un GuardDuty filtro Amazon, recuperare e un GuardDuty IPSet, recuperare un Set, recuperare e GuardDuty gli account dei membri, ottenere un GuardDuty ThreatIntel elenco di GuardDuty filtri, ottenere gli IPSet del GuardDuty servizio, recuperare i tag per il Servizio e ottenere il GuardDuty servizio; per ottenere lo stato e le impostazioni ThreatIntelSets di configurazione correnti per un account Amazon Macie; per recuperare le risorse e le associazioni principali per AWS Resource Access Manager (AWS RAM) le condivisioni di risorse e recuperare i dettagli sulle condivisioni di risorse; GuardDuty AWS RAM otten ere informazioni su un set di	

Modifica	Descrizione	Data
	configurazione esistente di Amazon Simple Email Service (Amazon SES), ottenere un elenco di destinazioni di eventi associate a un set di configurazione Amazon SES ed elencare tutti i set di configurazione associati a un account Amazon SES; e per ottenere un elenco degli attributi di directory di Identity Center, ottieni i dettagli di un set di AWS IAM Identity Center autorizzazioni, ottieni la policy gestita IAM allegata a un set di autorizzazioni IAM Identity Center specificato, get i permessi impostati per un'istanza di IAM Identity Center e ottieni i tag per IAM Identity Center risorse.	

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	Questa policy ora concede l'autorizzazione a ottenere un catalogo dati Amazon Athena specifico, elencare i cataloghi di dati Athena in Account AWS un ed elencare i tag associati a un gruppo di lavoro o a una risorsa del catalogo dati Athena; ottenere un elenco di grafici comportamentali di Amazon Detective e tag di elenco per un grafico di comportamento di Detective; ottenere un elenco di metadati di risorse per un determinato elenco di nomi di endpoint di sviluppo, ottenere informazioni su un endpoint AWS Glue di sviluppo specificato, ottieni tutti gli endpoint di sviluppo in un file, recupera una sicurezza AWS Glue specificata AWS Glue Account AWS AWS Glue configurazione, ottieni tutte le configurazioni di AWS Glue sicurezza, ottieni un elenco di tag associati a una AWS Glue risorsa, ottieni informazioni su un AWS Glue gruppo di lavoro con il nome specificato, recupera i nomi di tutte le risorse AWS Glue crawler in un AWS account, ottieni i nomi di tutte le AWS Glue	31 maggio 2022

Modifica	Descrizione	Data
scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	`DevEndpoint` risorse in un Account AWS, elenca i nomi di tutte le risorse di AWS Glue lavoro in un Account AWS, ottieni dettagli sugli account AWS Glue membro, elenca i nomi dei AWS Glue flussi di lavoro creati in un account ed elenca i AWS Glue gruppi di lavoro disponibili per un account; recuperare e dettagli su un GuardDuty filtro Amazon, recuperare e un GuardDuty IPSet, recuperare un Set, recuperare e GuardDuty gli account dei membri, ottenere un GuardDuty ThreatIntel elenco di GuardDuty filtri, ottenere gli IPSet del GuardDuty servizio, recuperare i tag per il Servizio e ottenere il GuardDuty servizio; per ottenere lo stato e le impostazioni ThreatIntelSets di configurazione correnti per un account Amazon Macie; per recuperare le risorse e le associazioni principali per AWS Resource Access Manager (AWS RAM) le condivisioni di risorse e recuperare i dettagli sulle condivisioni di risorse; GuardDuty AWS RAM otten ere informazioni su un set di	

Modifica	Descrizione	Data
	configurazione esistente di Amazon Simple Email Service (Amazon SES), ottenere un elenco di destinazioni di eventi associate a un set di configurazione Amazon SES ed elencare tutti i set di configurazione associati a un account Amazon SES; e per ottenere un elenco degli attributi di directory di Identity Center, ottieni i dettagli di un set di AWS IAM Identity Center autorizzazioni, ottieni la policy gestita IAM allegata a un set di autorizzazioni IAM Identity Center specificato, get i permessi impostati per un'istanza di IAM Identity Center e ottieni i tag per IAM Identity Center risorse.	

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	Questa politica ora consente di ottenere informazioni su tutti gli Event Data Store (EDS) o su uno specifico AWS CloudTrail Event Data Store (EDS), ottenere informazioni su tutte le risorse o su una determinata AWS CloudFormation risorsa, ottenere un elenco di un gruppo di parametri o sottoreti di DynamoDB Accelerator (DAX), ottenere informazioni AWS Database Migration Service sulle AWS DMS() attività di replica per l'account nell'area corrente a cui si accede e ottenere un elenco di tutte le politiche di un tipo specificato. AWS Organizations	7 aprile 2022

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	Questa politica ora consente di ottenere informazioni su tutti gli Event Data Store (EDS) o su uno specifico AWS CloudTrail Event Data Store (EDS), ottenere informazioni su tutte le risorse o su una determinata AWS CloudFormation risorsa, ottenere un elenco di un gruppo di parametri o sottoreti di DynamoDB Accelerator (DAX), ottenere informazioni AWS Database Migration Service sulle AWS DMS() attività di replica per l'account nell'area corrente a cui si accede e ottenere un elenco di tutte le politiche di un tipo specificato. AWS Organizations	7 aprile 2022

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara	Questa policy ora supporta autorizzazioni aggiuntive per AWS Backup, DynamoDB Accelerator AWS Batch, Amazon DynamoDB AWS Database Migration Service, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon FSx, Amazon,, Amazon Relational Database Service, V2 e Amazon. GuardDuty AWS Key Management Service AWS OpsWorks AWS WAF WorkSpaces	14 marzo 2022

Modifica	Descrizione	Data
meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterParameters, states:DescribeAct	Questa policy ora supporta autorizzazioni aggiuntive per AWS Backup, DynamoDB Accelerator AWS Batch, Amazon DynamoDB AWS Database Migration Service, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon FSx, Amazon,, Amazon Relational Database Service, V2 e Amazon. GuardDuty AWS Key Management Service AWS OpsWorks AWS WAF WorkSpaces	14 marzo 2022

Modifica	Descrizione	Data
ivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta di elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	Questa policy ora concede l'autorizzazione a ottenere dettagli sugli ambienti Elastic Beanstalk e una descrizione delle impostazioni per il set di configurazione Elastic Beanstalk specificato, ottenere una mappa delle nostre versioni di Elasticsearch, descrivere i gruppi di opzioni OpenSearch di Amazon RDS disponibili per un database e ottenere informazioni su una configurazione di distribuzione. CodeDeploy Questa policy ora concede anche l'autorizzazione a recuperare il contatto alternativo specificato allegato a una Account AWS, recuperare informazioni su una policy, recuperare una AWS Organizations policy del repository Amazon ECR, recuperare informazioni su una AWS Config regola archiviata, recuperare un elenco di famiglie di definizioni di attività Amazon ECS, elencare le unità organizzative (OU) principali o principali dell'unità organizzativa o dell'account figlio specificato ed elencare le politiche collegate alla radice, all'unità	10 febbraio 2022

Modifica	Descrizione	Data
	organizzativa o all'account di destinazione specificati.	

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	Questa policy ora concede l'autorizzazione a ottenere dettagli sugli ambienti Elastic Beanstalk e una descrizione delle impostazioni per il set di configurazione Elastic Beanstalk specificato, ottenere una mappa delle nostre versioni di Elasticsearch, descrivere i gruppi di opzioni OpenSearch di Amazon RDS disponibili per un database e ottenere informazioni su una configurazione di distribuzione. CodeDeploy Questa policy ora concede anche l'autorizzazione a recuperare il contatto alternativo specificato allegato a una Account AWS, recuperare informazioni su una policy, recuperare una AWS Organizations policy del repository Amazon ECR, recuperare informazioni su una AWS Config regola archiviata, recuperare un elenco di famiglie di definizioni di attività Amazon ECS, elencare le unità organizzative (OU) principali o principali dell'unità organizzativa o dell'account figlio specificato ed elencare le politiche collegate alla radice, all'unità	10 febbraio 2022

Modifica	Descrizione	Data
	organizzativa o all'account di destinazione specificati.	
AWSConfigServiceRolePolicy: aggiunta di logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	Questa politica ora concede l'autorizzazione a creare gruppi e flussi di CloudWatch log Amazon e a scrivere log su flussi di log creati.	15 dicembre 2021
AWS_ConfigRole: aggiunta di logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	Questa politica ora concede l'autorizzazione a creare gruppi e flussi di CloudWatch log Amazon e a scrivere log su flussi di log creati.	15 dicembre 2021
AWSConfigServiceRolePolicy: aggiunta di es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	Questa policy ora concede l'autorizzazione a ottenere dettagli su uno o più domini Amazon OpenSearch Service (OpenSearch Service) e a ottenere un elenco dettagliato dei parametri per un particolare gruppo di parametri DB di Amazon Relational Database Service (Amazon RDS). Questa politica concede inoltre l'autorizzazione a ottenere dettagli sugli snapshot di Amazon ElastiCache .	8 settembre 2021

Modifica	Descrizione	Data
AWS_ConfigRole: aggiunta di es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	Questa policy ora concede l'autorizzazione a ottenere dettagli su uno o più domini Amazon OpenSearch Service (OpenSearch Service) e a ottenere un elenco dettagliato dei parametri per un particolare gruppo di parametri DB di Amazon Relational Database Service (Amazon RDS). Questa politica concede inoltre l'autorizzazione a ottenere dettagli sugli snapshot di Amazon ElastiCache .	8 settembre 2021

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy— Aggiungere e aggiungere logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine autorizzazioni aggiuntive per i tipi di risorse AWS	Questa policy ora concede l'autorizzazione per elencare i tag per un gruppo di log, elencare i tag per una macchina a stati ed elencare tutte le macchine a stati. Questa policy ora concede l'autorizzazione per ottenere i dettagli su una macchina a stati. Questa policy ora supporta anche autorizzazioni aggiuntive per Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon, Amazon Simple Notification Service,, e. SageMaker AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway	28 luglio 2021

Modifica	Descrizione	Data
AWS_ConfigRole— AWS Aggiungi l e autorizzazioni aggiuntive per i tipi di risorse ogs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine	Questa policy ora concede l'autorizzazione per elencare i tag per un gruppo di log, elencare i tag per una macchina a stati ed elencare tutte le macchine a stati. Questa policy ora concede l'autorizzazione per ottenere i dettagli su una macchina a stati. Questa policy ora supporta anche autorizzazioni aggiuntive per Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon, Amazon Simple Notification Service,, e. SageMaker AWS Database Migration Service A WS Global Accelerator AWS Storage Gateway	28 luglio 2021

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy— ssm:DescribeDocumentPermission Aggiungere e aggiungere AWS autorizzazioni aggiuntive per i tipi di risorse	Questa policy ora concede l'autorizzazione per visualizzare le autorizzazioni dei documenti AWS Systems Manager e le informazioni su IAM Access Analyzer. Questa policy ora supporta tipi di AWS risorse aggiuntivi per Amazon Kinesis, Amazon, ElastiCache Amazon EMR, Amazon Route 53 e AWS Network Firewall Amazon Relational Database Service (Amazon RDS). Queste modifiche alle autorizzazioni consentono di AWS Config richiamare le API di sola lettura necessarie per supportare questi tipi di risorse. Questa policy ora supporta anche il filtraggio delle funzioni Lambda @Edge per la regola gestita AWS Config lambda-inside-vpc.	8 giugno 2021

Modifica	Descrizione	Data
AWS_ConfigRole— Aggiungere e aggiungere autorizzazioni aggiuntive per i tipi di risorse ssm:DescribeDocumentPermission AWS	Questa policy ora concede l'autorizzazione per visualizzare le autorizzazioni dei documenti AWS Systems Manager e le informazioni su IAM Access Analyzer. Questa policy ora supporta tipi di AWS risorse aggiuntivi per Amazon Kinesis, Amazon, ElastiCache Amazon EMR, Amazon Route 53 e AWS Network Firewall Amazon Relational Database Service (Amazon RDS). Queste modifiche alle autorizzazioni consentono di AWS Config richiamare le API di sola lettura necessarie per supportare questi tipi di risorse. Questa policy ora supporta anche il filtraggio delle funzioni Lambda @Edge per la regola gestita AWS Config lambda-inside-vpc.	8 giugno 2021

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy: aggiunta dell'autorizzazione apigateway:GET per effettuare chiamate GET di sola lettura a Gateway API e delle autorizzazioni s3:GetAccessPointPolicy e s3:GetAccessPointPolicyStatus per richiamare le API di sola lettura di Amazon S3	Questa politica ora concede autorizzazioni che consentono di effettuare chiamate GET di sola lettura AWS Config ad API Gateway per supportare una AWS Config regola per API Gateway. La policy aggiunge anche autorizzazioni che consentono di AWS Config richiamare le API di sola lettura di Amazon Simple Storage Service (Amazon S3), necessarie per supportare il nuovo tipo di risorsa. `AWS::S3::AccessPoint`	10 maggio 2021
AWS_ ConfigRole — Aggiungi apigateway:GET l'autorizzazione per effettuare chiamate GET di sola lettura verso API Gateway e l's3:GetAccessPointPolicyautorizzazione e s3:GetAccessPointPolicyStatus l'autorizzazione per richiamare le API di sola lettura di Amazon S3	Questa politica ora concede autorizzazioni che consentono di effettuare chiamate GET di sola lettura AWS Config ad API Gateway per supportare un for API Gateway. AWS Config La policy aggiunge anche autorizzazioni che consentono di AWS Config richiamare le API di sola lettura di Amazon Simple Storage Service (Amazon S3), necessarie per supportare il nuovo tipo di risorsa. `AWS::S3::AccessPoint`	10 maggio 2021

Modifica	Descrizione	Data
AWSConfigServiceRolePolicy— Aggiungere ssm:ListDocuments autorizzazioni e autorizzazioni aggiuntive per i tipi di risorse AWS	Questa policy ora concede l'autorizzazione per visualizzare le informazioni relative ai documenti AWS Systems Manager specificati. Questa policy ora supporta anche tipi di AWS risorse aggiuntivi per AWS Backup Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon SageMaker AWS Database Migration Service Kinesis, Amazon e Amazon Route 53. Queste modifiche alle autorizzazioni consentono di AWS Config richiamare le API di sola lettura necessarie per supportare questi tipi di risorse.	1 aprile 2021

Modifica	Descrizione	Data
AWS_ConfigRole— Aggiungere ssm:ListDocuments autorizzazioni e autorizzazioni aggiuntive per i tipi di risorse AWS	Questa policy ora concede l'autorizzazione per visualizzare le informazioni relative ai documenti AWS Systems Manager specificati. Questa policy ora supporta anche tipi di AWS risorse aggiuntivi per AWS Backup Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon SageMaker AWS Database Migration Service Kinesis, Amazon e Amazon Route 53. Queste modifiche alle autorizzazioni consentono di AWS Config richiamare le API di sola lettura necessarie per supportare questi tipi di risorse.	1 aprile 2021
`AWSConfigRole` è obsoleta	`AWSConfigRole` è obsoleta La policy sostitutiva è `AWS_ConfigRole` .	1 aprile 2021
AWS Config ha iniziato a tenere traccia delle modifiche	AWS Config ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	1 aprile 2021

Autorizzazioni per il ruolo IAM assegnato a AWS Config

Un ruolo IAM ti consente di definire un set di autorizzazioni. AWS Config assume il ruolo che gli assegni per scrivere nel tuo bucket S3, pubblicare sul tuo argomento SNS ed effettuare richieste `List` API per ottenere i dettagli di `Describe` configurazione delle tue risorse. AWS Per ulteriori informazioni sui ruoli IAM, consulta Ruoli IAM nella Guida per l'utente di IAM.

Quando utilizzi la AWS Config console per creare o aggiornare un ruolo IAM, ti assegna AWS Config automaticamente le autorizzazioni necessarie. Per ulteriori informazioni, consulta Configurazione AWS Config con la console.

Indice

- Creazione di policy del ruolo IAM
  - Aggiunta di una policy di attendibilità IAM al ruolo
  - Policy del ruolo IAM per il bucket S3
  - Policy del ruolo IAM per la chiave KMS
  - Policy del ruolo IAM per un argomento Amazon SNS
  - Policy del ruolo IAM per il recupero dei dettagli di configurazione
- Gestione delle autorizzazioni per la registrazione dei bucket S3

Creazione di policy del ruolo IAM

Quando utilizzi la AWS Config console per creare un ruolo IAM, assegna AWS Config automaticamente le autorizzazioni necessarie al ruolo.

Se utilizzi il AWS CLI per configurare AWS Config o stai aggiornando un ruolo IAM esistente, devi aggiornare manualmente la policy per consentire l'accesso AWS Config al tuo bucket S3, la pubblicazione sul tuo argomento SNS e ottenere dettagli di configurazione sulle tue risorse.

Aggiunta di una policy di attendibilità IAM al ruolo

Puoi creare una policy di fiducia IAM che AWS Config consenta di assumere un ruolo e utilizzarlo per tenere traccia delle tue risorse. Per ulteriori informazioni sulle policy di attendibilità, consulta Termini e concetti dei ruoli nella Guida per l'utente di IAM.

Di seguito è riportato un esempio di policy di fiducia per AWS Config i ruoli:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

Puoi utilizzare la condizione `AWS:SourceAccount` nella relazione di trust del ruolo IAM riportata sopra per fare in modo che il principale del servizio Config interagisca con il ruolo AWS IAM solo quando esegue operazioni per conto di account specifici.

AWS Config supporta anche la `AWS:SourceArn` condizione che limita il principale del servizio Config ad assumere il ruolo IAM solo quando esegue operazioni per conto dell'account proprietario. Quando si utilizza il AWS Config service principal, la `AWS:SourceArn` proprietà verrà sempre impostata su `arn:aws:config:sourceRegion:sourceAccountID:*` dove si `sourceRegion` trova la regione del registratore di configurazione e `sourceAccountID` sull'ID dell'account contenente il registratore di configurazione. Per ulteriori informazioni sul Registratore di AWS Config configurazione, vedere Gestione del registratore di configurazione. Ad esempio, aggiungi la seguente condizione che limita il principale del servizio Config in modo che assuma il ruolo IAM solo per conto di un registratore di configurazione nella regione `us-east-1` dell'account `123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Policy del ruolo IAM per il bucket S3

La seguente politica di esempio concede l' AWS Config autorizzazione ad accedere al bucket S3:

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
```

```
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":[
        "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::myBucketName"
    }
  ]
}
```

Policy del ruolo IAM per la chiave KMS

La seguente policy di esempio concede l' AWS Config autorizzazione a utilizzare la crittografia basata su KMS su nuovi oggetti per la distribuzione di bucket S3:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN"
        }
    ]
}
```

Policy del ruolo IAM per un argomento Amazon SNS

La seguente politica di esempio concede l' AWS Config autorizzazione ad accedere all'argomento SNS:

```
{
  "Version": "2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"mySNStopicARN"
     }
    ]
}
```

Se l'argomento SNS è crittografato per istruzioni di configurazione aggiuntive, consulta Configurazione delle autorizzazioni per AWS KMS nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Policy del ruolo IAM per il recupero dei dettagli di configurazione

Per registrare le configurazioni AWS delle risorse, sono AWS Config necessarie le autorizzazioni IAM per ottenere i dettagli di configurazione delle risorse.

Utilizza la policy AWS gestita AWS_ ConfigRole e collegala al ruolo IAM a cui assegni. AWS Config AWS aggiorna questa politica ogni volta che AWS Config aggiunge il supporto per un tipo di AWS risorsa, il che significa che AWS Config continuerà ad avere le autorizzazioni necessarie per ottenere i dettagli di configurazione purché al ruolo sia associata questa politica gestita.

Se crei o aggiorni un ruolo con la console, AWS Config collega ConfigRoleAWS_ al posto tuo.

Se usi il AWS CLI, usa il **`attach-role-policy`** comando e specifica l'Amazon Resource Name (ARN) per AWS_: ConfigRole

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn
 arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
```

Gestione delle autorizzazioni per la registrazione dei bucket S3

AWS Config registra e invia notifiche quando un bucket S3 viene creato, aggiornato o eliminato.

Si consiglia di utilizzare il ruolo `AWSServiceRoleForConfig` (consulta Utilizzo di ruoli collegati ai servizi per AWS Config) o un ruolo IAM personalizzato tramite la policy gestita `AWS_ConfigRole`. Per ulteriori informazioni sulle best practice per la registrazione della configurazione, consulta Best practice di AWS Config.

Se devi gestire le autorizzazioni a livello di oggetto per la registrazione del bucket, assicurati che nella policy del bucket S3 sia possibile fornire `config.amazonaws.com` (il nome principale del AWS Config servizio) l'accesso a tutte le autorizzazioni relative a S3 previste dalla policy gestita. `AWS_ConfigRole` Per ulteriori informazioni, consulta Autorizzazioni per il bucket Amazon S3.

Aggiornamento del ruolo IAM assegnato a AWS Config

Puoi aggiornare il ruolo IAM assunto in AWS Config qualsiasi momento. Prima di aggiornare il ruolo IAM, assicurati di aver creato un nuovo ruolo che sostituisca il precedente. Devi allegare al nuovo ruolo delle policy che concedono le autorizzazioni per AWS Config registrare le configurazioni e distribuirle al tuo canale di distribuzione. Inoltre, assicurati di annotare il nome della risorsa Amazon (ARN) del nuovo ruolo IAM. Avrai bisogno di tale informazione per aggiornare il ruolo IAM. Per ulteriori informazioni su come creare un ruolo IAM e collegarvi le relative policy richieste, consulta Creazione di un ruolo IAM.

> **Note**
>
> Per trovare l'ARN di un ruolo IAM esistente, vai alla console IAM all'indirizzo https://console.aws.amazon.com/iam/. Nel riquadro di navigazione scegliere Roles (Ruoli). Quindi scegliere il nome del ruolo desiderato e individuare l'ARN nella parte superiore della pagina di Riepilogo.

Aggiornamento del ruolo IAM

Puoi aggiornare il tuo ruolo IAM utilizzando AWS Management Console o il. AWS CLI

To update the IAM role (Console)

Se lo utilizzi AWS Config in una regione che supporta AWS Config le regole, completa i seguenti passaggi. Per un elenco delle regioni supportate, consultaRegioni ed endpoint di AWS Config nei Riferimenti generali di Amazon Web Services.

1. Accedi AWS Management Console e apri la AWS Config console all'indirizzo https://console.aws.amazon.com/config/.
2. Scegliere Settings (Impostazioni) nel riquadro di navigazione.
3. Scegli Modifica nella pagina Impostazioni.
4. Nella sezione Governance dei dati, scegli il ruolo IAM per AWS Config:
   - Usa un ruolo esistente AWS Config collegato al servizio: AWS Config crea un ruolo con le autorizzazioni richieste.
   - Scegli un ruolo dal tuo account: per i ruoli esistenti, scegli un ruolo IAM nel tuo account.
5. Selezionare Salva.

To update the IAM role (AWS CLI)

Utilizzare il comando `put-configuration-recorder` e specificare l'Amazon Resource Name (ARN) del nuovo ruolo:

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

Autorizzazioni per il bucket Amazon S3 per il canale di distribuzione AWS Config

> **Important**
>
> Questa pagina riguarda la configurazione di Amazon S3 Bucket per il AWS Config canale di distribuzione. Questa pagina non riguarda il tipo di `AWS::S3::Bucket` risorsa che il registratore di AWS Config configurazione può registrare. Per ulteriori informazioni sul canale di AWS Config consegna, consulta Gestione del canale di consegna.

Per impostazione predefinita, tutti gli oggetti e i bucket Amazon S3 sono privati. Solo il proprietario della risorsa Account AWS che ha creato il bucket può accedervi. Tuttavia, il proprietario della risorsa può concedere ad altre risorse e utenti le autorizzazioni di accesso. Un modo per farlo è scrivere una policy d'accesso.

Se AWS Config crea automaticamente un bucket Amazon S3 per te (ad esempio, se utilizzi la AWS Config console per configurare il canale di distribuzione), queste autorizzazioni vengono aggiunte automaticamente al bucket Amazon S3. Tuttavia, se specifichi un bucket Amazon S3 esistente, devi accertarti che il bucket S3 disponga delle autorizzazioni corrette.

> **Note**
>
> Un oggetto non eredita le autorizzazioni dal bucket a cui appartiene. Se ad esempio si crea un bucket e si concede l'accesso in scrittura a un utente, non sarà possibile accedere agli oggetti di tale utente a meno che questi non conceda esplicitamente l'accesso.

Indice

- Autorizzazioni richieste per il bucket Amazon S3 quando si usano i ruoli IAM
- Autorizzazioni richieste per il bucket Amazon S3 quando si usano i ruoli collegati ai servizi
- Concessione dell' AWS Config accesso al bucket Amazon S3

Autorizzazioni richieste per il bucket Amazon S3 quando si usano i ruoli IAM

Quando AWS Config invia informazioni di configurazione (file di cronologia e istantanee) al bucket Amazon S3 nel tuo account, assume il ruolo IAM che hai assegnato al momento della configurazione. AWS Config Quando AWS Config invia le informazioni di configurazione a un bucket Amazon S3 in un altro account, prova prima di tutto a utilizzare il ruolo IAM, ma questo tentativo ha esito negativo se la policy di accesso per il bucket non concede l'accesso `WRITE` al ruolo IAM. In questo caso, AWS Config invia nuovamente le informazioni, questa volta come responsabile del servizio. AWS Config Prima che la consegna possa avere successo, la politica di accesso deve concedere l'`WRITE`accesso al nome `config.amazonaws.com` principale. AWS Config è quindi il proprietario degli oggetti che consegna al bucket S3. Per concedere ad AWS Config l'accesso al bucket Amazon S3, devi collegare al bucket Amazon S3 di un altro account una policy di accesso, come indicato al passaggio 6 qui di seguito.

Before AWS Config can delivery dei log al tuo AWS Config bucket Amazon S3 verifica se il bucket esiste e in AWS quale regione si trova. AWS Config tenta di chiamare l'HeadBucketAPI Amazon S3 per verificare se il bucket esiste e per ottenere la regione del bucket. Se non vengono fornite le autorizzazioni per localizzare il bucket quando viene eseguito il controllo della posizione, viene visualizzato un errore nei log. `AccessDenied` AWS CloudTrail Tuttavia, la distribuzione del log al bucket Amazon S3 va a buon fine se non fornisci le autorizzazioni per la posizione del bucket.

> **Note**
>
> Per consentire l'autorizzazione per l'API `HeadBucket` di Amazon S3, fornisci l'autorizzazione per eseguire l'azione `s3:ListBucket` come `SidAWSConfigBucketExistenceCheck`, menzionata nel passaggio 6 di seguito.

Autorizzazioni richieste per il bucket Amazon S3 quando si usano i ruoli collegati ai servizi

Il ruolo AWS Config collegato al servizio non dispone dell'autorizzazione per inserire oggetti nei bucket Amazon S3. Pertanto, se configuri AWS Config utilizzando un ruolo collegato al servizio, AWS Config invierà invece gli elementi di configurazione come principale del servizio. AWS Config Dovrai allegare una politica di accesso, menzionata nel passaggio 6 di seguito, al bucket Amazon S3 del tuo account o a un altro account per concedere AWS Config l'accesso al bucket Amazon S3.

Concessione dell' AWS Config accesso al bucket Amazon S3

Segui questi passaggi per aggiungere una policy di accesso al bucket Amazon S3 nel tuo account o in un altro account. La policy di accesso consente di AWS Config inviare informazioni di configurazione a un bucket Amazon S3.

1. Accedi AWS Management Console utilizzando l'account che ha il bucket S3.
2. Apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
3. Seleziona il bucket che desideri utilizzare AWS Config per fornire gli elementi di configurazione, quindi scegli Proprietà.
4. Seleziona Autorizzazioni.
5. Scegliere Edit Bucket Policy (Modifica policy bucket).
6. Copiare la seguente policy nella finestra Bucket Policy Editor (Editor policy del bucket).

> **Important**
>
> Come best practice di sicurezza per consentire l' AWS Config accesso a un bucket Amazon S3, consigliamo vivamente di limitare l'accesso nella policy del bucket con la condizione. `AWS:SourceAccount` Se la tua policy sui bucket esistente non segue questa best practice di sicurezza, ti consigliamo vivamente di modificarla per includere

questa protezione. In questo modo AWS Config viene garantito l'accesso solo per conto degli utenti previsti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::targetBucketName",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::targetBucketName",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
```

```
      "Resource": "arn:aws:s3:::targetBucketName/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

> **Note**
>
> Quando concedi le autorizzazioni al tuo ruolo IAM anziché al nome principale del AWS Config servizio (SPN), assicurati che il tuo ruolo IAM disponga dell'`PutObjectACL`autorizzazione sul bucket tra account per evitare errori di autorizzazione insufficienti. Alla sezione Policy del ruolo IAM per il bucket S3 puoi trovare un esempio di policy del ruolo IAM.

7. Sostituire i seguenti valori nella policy del bucket:
   - *`target BucketName`*: il nome del bucket Amazon S3 a cui AWS Config verranno consegnati gli elementi di configurazione.
   - *`[optional] prefix`*: un'aggiunta opzionale alla chiave dell'oggetto Amazon S3 che aiuta a creare, all'interno del bucket, un'organizzazione a cartelle.
   - *`sourceAccountID`*: l'ID dell'account per il quale AWS Config verranno consegnati gli elementi di configurazione al bucket di destinazione.
8. Scegliere Save (Salva) e Close (Chiudi).

Puoi utilizzare la condizione `AWS:SourceAccount` nella policy del bucket Amazon S3 riportata sopra per fare in modo il principale del servizio Config interagisca con il bucket Amazon S3 solo quando esegue operazioni per conto di account specifici. Se prevedi di configurare AWS Config più account della stessa organizzazione per distribuire elementi di configurazione a un singolo bucket Amazon S3, ti consigliamo di utilizzare i ruoli IAM anziché i ruoli collegati ai servizi in modo da poter utilizzare AWS Organizations chiavi di condizioni come. `AWS:PrincipalOrgID` Per ulteriori informazioni sulla gestione delle autorizzazioni di accesso per un ruolo IAM con cui utilizzare AWS Config, consulta Autorizzazioni per il ruolo IAM assegnato a. AWS Config Per ulteriori informazioni

sulla gestione delle autorizzazioni di accesso per AWS Organizations, consulta Gestione delle autorizzazioni di accesso per la tua organizzazione. AWS

AWS Config supporta anche la `AWS:SourceArn` condizione che limita il principale del servizio Config a interagire solo con il bucket Amazon S3 quando esegue operazioni per conto di canali di distribuzione specifici. AWS Config Quando si utilizza l'entità del AWS Config servizio, la `AWS:SourceArn` proprietà verrà sempre impostata su `arn:aws:config:sourceRegion:sourceAccountID:*` dove si `sourceRegion` trova la regione del canale di consegna e `sourceAccountID` sull'ID dell'account contenente il canale di consegna. Per ulteriori informazioni sui canali AWS Config di distribuzione, consulta Gestione del canale di consegna. Ad esempio, aggiungi la seguente condizione per limitare il principale del servizio Config in modo che interagisca con il bucket Amazon S3 solo per conto di un canale di distribuzione nella regione `us-east-1` dell'account `123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Autorizzazioni per la chiave KMS per il AWS Config canale di consegna

Utilizza le informazioni contenute in questo argomento se desideri creare una policy per una AWS KMS chiave per il tuo bucket S3 che ti consenta di utilizzare la crittografia basata su KMS sugli oggetti forniti da per la consegna dei bucket S3. AWS Config

Indice

- Autorizzazioni richieste per la chiave KMS quando si utilizzano i ruoli IAM (distribuzione dei bucket S3)
- Autorizzazioni richieste per la AWS KMS chiave quando si utilizzano ruoli collegati ai servizi (S3 Bucket Delivery)
- Concessione dell' AWS Config accesso alla chiave AWS KMS

Autorizzazioni richieste per la chiave KMS quando si utilizzano i ruoli IAM (distribuzione dei bucket S3)

Se configuri AWS Config utilizzando un ruolo IAM, puoi allegare la seguente politica di autorizzazione alla chiave KMS:

```
{
    "Id": "Policy_ID",
```

```
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
        }
    ]
}
```

> **Note**
>
> Se il ruolo IAM, la policy del bucket Amazon S3 o la AWS KMS chiave non forniscono un accesso appropriato a AWS Config, il tentativo AWS Config di inviare le informazioni di configurazione al bucket Amazon S3 avrà esito negativo. In questo caso, AWS Config invia nuovamente le informazioni, questa volta come principale del servizio. AWS Config In questo caso, è necessario allegare una politica di autorizzazione, menzionata di seguito, alla AWS KMS chiave per concedere AWS Config l'accesso per utilizzare la chiave quando si forniscono informazioni al bucket Amazon S3.

Autorizzazioni richieste per la AWS KMS chiave quando si utilizzano ruoli collegati ai servizi (S3 Bucket Delivery)

Il ruolo AWS Config collegato al servizio non dispone dell'autorizzazione per accedere alla chiave. AWS KMS Pertanto, se configuri AWS Config l'utilizzo di un ruolo collegato al servizio, AWS Config invierà invece le informazioni come responsabile del AWS Config servizio. Dovrai allegare una politica di accesso, menzionata di seguito, alla AWS KMS chiave per concedere AWS Config l'accesso per utilizzare la AWS KMS chiave per fornire informazioni al bucket Amazon S3.

Concessione dell' AWS Config accesso alla chiave AWS KMS

Questa policy consente di AWS Config utilizzare una AWS KMS chiave per fornire informazioni a un bucket Amazon S3.

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

Sostituisci i seguenti valori nella policy della chiave:

- *`MyKMSKeyarn`*: l'ARN della chiave utilizzata per crittografare AWS KMS i dati nel bucket Amazon S3 a cui fornirà gli elementi di configurazione. AWS Config
- *`sourceAccountID`*: l'ID dell'account per il quale AWS Config distribuisce gli elementi di configurazione.

È possibile utilizzare la `AWS:SourceAccount` condizione nella politica AWS KMS chiave riportata sopra per limitare l'interazione del principale del servizio Config con la AWS KMS chiave solo durante l'esecuzione di operazioni per conto di account specifici.

AWS Config supporta anche la `AWS:SourceArn` condizione che limita il principale del servizio Config a interagire solo con il bucket Amazon S3 quando esegue operazioni

per conto di canali di distribuzione specifici. AWS Config Quando si utilizza l'entità del AWS Config servizio, la `AWS:SourceArn` proprietà verrà sempre impostata su `arn:aws:config:sourceRegion:sourceAccountID:*` dove si `sourceRegion` trova la regione del canale di consegna e `sourceAccountID` sull'ID dell'account contenente il canale di consegna. Per ulteriori informazioni sui canali AWS Config di distribuzione, consulta Gestione del canale di consegna. Ad esempio, aggiungi la seguente condizione per limitare il principale del servizio Config in modo che interagisca con il bucket Amazon S3 solo per conto di un canale di distribuzione nella regione `us-east-1` dell'account `123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Autorizzazioni per l'argomento Amazon SNS

Questo argomento descrive come configurare la distribuzione AWS Config di argomenti Amazon SNS di proprietà di un account diverso. AWS Config deve disporre delle autorizzazioni necessarie per inviare notifiche a un argomento di Amazon SNS. Per la configurazione dello stesso account, quando la AWS Config console crea un argomento Amazon SNS o scegli un argomento Amazon SNS dal tuo account AWS Config , assicurati che l'argomento Amazon SNS includa le autorizzazioni richieste e segua le best practice di sicurezza.

> **Note**
>
> AWS Config attualmente supporta solo l'accesso nella stessa regione e tra più account. Gli argomenti SNS utilizzati per i documenti di riparazione AWS Systems Manager (SSM) o per il canale di distribuzione del registratore non possono essere interregionali.

Indice

- Autorizzazioni richieste per l'argomento Amazon SNS quando si usano i ruoli IAM
- Autorizzazioni richieste per l'argomento Amazon SNS quando si utilizzano i ruoli collegati ai servizi
- Concessione dell' AWS Config accesso all'argomento Amazon SNS.
- Risoluzione dei problemi legati agli argomenti Amazon SNS

Autorizzazioni richieste per l'argomento Amazon SNS quando si usano i ruoli IAM

Puoi collegare una policy di autorizzazione all'argomento Amazon SNS di proprietà di un altro account. Se desideri utilizzare un argomento Amazon SNS di un altro account, assicurati di collegare la seguente policy all'argomento Amazon SNS esistente.

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

Nella chiave `Resource`, *`account-id`* corrisponde al numero di account AWS del proprietario dell'argomento. Per *`account-id1`*, *`account-id2 e account-id3`*, usa quello che Account AWS invierà i dati a un argomento di Amazon SNS. Puoi sostituire i valori appropriati per i parametri *`region`* e *`myTopic`*.

Quando AWS Config invia una notifica a un argomento Amazon SNS, tenta innanzitutto di utilizzare il ruolo IAM, ma questo tentativo fallisce se il ruolo o Account AWS non dispone dell'autorizzazione per pubblicare sull'argomento. In questo caso, AWS Config invia nuovamente la notifica, questa volta come nome principale AWS Config del servizio (SPN). Prima che la pubblicazione possa andare a buon fine, la policy di accesso per l'argomento deve concedere l'accesso `sns:Publish` al nome del principale `config.amazonaws.com`. È necessario collegare una policy di accesso, descritta nella sezione successiva, all'argomento Amazon SNS per concedere ad AWS Config l'accesso all'argomento Amazon SNS se il ruolo IAM non è autorizzato a pubblicare sull'argomento.

Autorizzazioni richieste per l'argomento Amazon SNS quando si utilizzano i ruoli collegati ai servizi

Il ruolo AWS Config collegato al servizio non dispone dell'autorizzazione per accedere all'argomento Amazon SNS. Quindi, se configuri AWS Config utilizzando un ruolo collegato al servizio (SLR), AWS

Config invierà invece le informazioni come responsabile del servizio. AWS Config Dovrai allegare una politica di accesso, menzionata di seguito, all'argomento Amazon SNS per concedere AWS Config l'accesso all'invio di informazioni all'argomento Amazon SNS.

Per la configurazione nello stesso account, quando l'argomento Amazon SNS e il ruolo SLR si trovano nello stesso account e la policy di Amazon SNS concede l'autorizzazione "`sns:Publish`" dell'SLR, non è necessario utilizzare l'SPN AWS Config . La policy di autorizzazione riportata di seguito e le raccomandazioni sulle best practice di sicurezza riguardano la configurazione tra più account.

Concessione dell' AWS Config accesso all'argomento Amazon SNS.

Questa politica consente di AWS Config inviare una notifica a un argomento di Amazon SNS. Per concedere AWS Config l'accesso all'argomento Amazon SNS da un altro account, dovrai allegare la seguente politica di autorizzazione.

> **Note**
>
> Come best practice in materia di sicurezza, si consiglia vivamente di assicurarsi che AWS Config acceda alle risorse per conto degli utenti previsti solo limitando l'accesso agli account indicati nelle condizioni. `AWS:SourceAccount`

```
{
"Id": "Policy_ID",
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
```

```
        }
      }
    }
  ]
}
```

Nella chiave `Resource`, *`account-id`* corrisponde al numero di account AWS del proprietario dell'argomento. Per *`account-id1`*, *`account-id2 e account-id3`*, usa quello che Account AWS invierà i dati a un argomento di Amazon SNS. Puoi sostituire i valori appropriati per i parametri *`region`* e *`myTopic`*.

Puoi utilizzare la `AWS:SourceAccount` condizione della precedente policy tematica di Amazon SNS per limitare l'interazione del nome principale del AWS Config servizio (SPN) solo con l'argomento Amazon SNS durante l'esecuzione di operazioni per conto di account specifici.

AWS Config supporta anche la `AWS:SourceArn` condizione che limita il nome principale del AWS Config servizio (SPN) all'interazione con il bucket S3 solo quando si eseguono operazioni per conto di canali di distribuzione specifici. AWS Config Quando si utilizza il nome principale del AWS Config servizio (SPN), la `AWS:SourceArn` proprietà verrà sempre impostata su `arn:aws:config:sourceRegion:sourceAccountID:*` dove si `sourceRegion` trova la regione del canale di consegna e `sourceAccountID` sull'ID dell'account contenente il canale di consegna. Per ulteriori informazioni sui canali di AWS Config distribuzione, consulta Gestione del canale di consegna. Ad esempio, aggiungi la seguente condizione per limitare l'interazione del nome principale del AWS Config servizio (SPN) con il tuo bucket S3 solo per conto di un canale di distribuzione nella `us-east-1` regione dell'account:. `123456789012` `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`

Risoluzione dei problemi legati agli argomenti Amazon SNS

AWS Config deve disporre delle autorizzazioni per inviare notifiche a un argomento di Amazon SNS. Se un argomento Amazon SNS non può ricevere notifiche, verifica che il ruolo IAM che AWS Config stava assumendo disponga delle autorizzazioni richieste. `sns:Publish`

Risoluzione dei problemi AWS Config di identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con un AWS Config IAM.

Argomenti

- Non sono autorizzato a eseguire alcuna azione in AWS Config
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS Config risorse

Non sono autorizzato a eseguire alcuna azione in AWS Config

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` IAM prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `config:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 config:GetWidget on resource: my-example-widget
```

In questo caso, la policy deve essere aggiornata in modo che Mateo possa accedere alla risorsa *`my-example-widget`* mediante l'operazione `config:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a AWS Config.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS Config. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS Config risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Config supporta queste funzionalità, consultaCome AWS Config funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per scoprire la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Utilizzo dei ruoli collegati ai servizi per AWS Config

AWS Config utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS Config I ruoli collegati ai servizi sono predefiniti AWS Config e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione AWS Config perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Config definisce le autorizzazioni dei

ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS Config Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni relative ai ruoli collegati al servizio per AWS Config

AWS Config utilizza il ruolo collegato al servizio denominato AWSServiceRoleForConfig: AWS Config utilizza questo ruolo collegato al servizio per chiamare altri servizi per conto dell'utente. AWS

Il ruolo AWSServiceRoleForConfigcollegato al servizio si fida che il servizio assuma il ruolo. `config.amazonaws.com`

La politica di autorizzazione per il `AWSServiceRoleForConfig` ruolo contiene autorizzazioni di sola lettura e di sola scrittura per le risorse e autorizzazioni di sola lettura per le AWS Config risorse di altri servizi che supportano. AWS Config Per visualizzare la politica gestita, vedere Politiche gestite per. AWSServiceRoleForConfigAWSAWS Config Per ulteriori informazioni, consulta Tipi di risorsa supportati.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Per utilizzare un ruolo collegato al servizio con AWS Config, devi configurare le autorizzazioni sul tuo bucket Amazon S3 e sull'argomento Amazon SNS. Per ulteriori informazioni, consulta Autorizzazioni richieste per il bucket Amazon S3 quando si usano i ruoli collegati ai servizi, Autorizzazioni richieste per la AWS KMS chiave quando si utilizzano ruoli collegati ai servizi (S3 Bucket Delivery) e Autorizzazioni richieste per l'argomento Amazon SNS quando si utilizzano i ruoli collegati ai servizi.

Creazione di un ruolo collegato ai servizi per AWS Config

Nella CLI IAM o nell'API IAM, crea un ruolo collegato ai servizi con il nome servizio `config.amazonaws.com`. Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato al servizio per AWS Config

AWS Config non consente di modificare il ruolo collegato al AWSServiceRoleForConfigservizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per AWS Config

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se il AWS Config servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare AWS Config le risorse utilizzate da AWSServiceRoleForConfig

Verificare che `ConfigurationRecorders` non stia utilizzano ruolo collegato ai servizi. È possibile utilizzare la AWS Config console per arrestare il registratore di configurazione. Per arrestare la registrazione, in La registrazione è attivata, scegli Disattiva.

È possibile eliminare l' AWS Config API in `ConfigurationRecorder` uso. Per eliminare, utilizza il comando `delete-configuration-recorder`.

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM, la CLI IAM o l'API IAM per eliminare il ruolo collegato al AWSServiceRoleForConfig servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Risposta agli incidenti in AWS Config

La sicurezza è la massima priorità in AWS. Come parte del modello di responsabilità condivisa del AWS cloud, AWS gestisce un data center, una rete e un'architettura software che soddisfa i requisiti delle organizzazioni più sensibili alla sicurezza. AWS è responsabile di qualsiasi risposta agli incidenti relativi al servizio stesso AWS Config . Inoltre, in qualità di AWS cliente, condividi la responsabilità di mantenere la sicurezza nel cloud. Ciò significa che controllate la sicurezza che scegliete di implementare utilizzando gli AWS strumenti e le funzionalità a cui avete accesso e siete responsabili della risposta agli incidenti dal punto di vista del modello di responsabilità condivisa.

Stabilendo una linea di base di sicurezza che soddisfi gli obiettivi delle applicazioni eseguite nel cloud, sei in grado di rilevare deviazioni a cui puoi rispondere. Poiché la risposta agli incidenti di sicurezza può essere un argomento complesso, ti invitiamo a consultare le seguenti risorse in modo da comprendere meglio l'impatto che la risposta agli incidenti (IR) e le tue scelte hanno sugli obiettivi aziendali: AWS Security Incident Response Guide, white paper sulle migliori pratiche di AWS sicurezza e white paper Security Perspective of the AWS Cloud Adoption Framework (CAF).

Convalida della conformità per AWS Config

I revisori esterni valutano la sicurezza e la conformità nell' AWS Config ambito di più programmi di AWS conformità. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.

- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Evaluating Resources with Rules nella AWS Config Developer Guide: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in AWS Config

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni offrono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire

applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS

Sicurezza dell'infrastruttura in AWS Config

In quanto servizio gestito, AWS Config è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere AWS Config attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Analisi della configurazione e delle vulnerabilità

Per AWS Config, AWS gestisce attività di sicurezza di base come l'applicazione di patch al sistema operativo (OS) guest e al database, la configurazione del firewall e il disaster recovery.

Prevenzione del confused deputy tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel frattempo AWS, l'impersonificazione tra servizi può portare al confuso problema del vicesceriffo. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio

chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Si consiglia di utilizzare `aws:SourceArn`le chiavi di contesto della condizione `aws:SourceAccount`globale nelle politiche delle risorse per limitare le autorizzazioni che AWS Config forniscono un altro servizio alla risorsa. Utilizza `aws:SourceArn` se desideri consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizza `aws:SourceAccount` se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn`con l'ARN completo della risorsa. Se non conosci l'ARN completo della risorsa o scegli più risorse, utilizza la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (`*`) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:servicename:*:123456789012:*`.

Se il valore `aws:SourceArn` non contiene l'ID account, ad esempio un ARN di un bucket Amazon S3, è necessario utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni.

L'esempio seguente mostra come utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition AWS Config per evitare il confuso problema vice: concedere AWS Config l'accesso al bucket Amazon S3.

Best practice di sicurezza per AWS Config

AWS Config fornisce una serie di funzionalità di sicurezza da considerare durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

- Sfrutta il tagging for AWS Config, che semplifica la gestione, la ricerca e il filtraggio delle risorse.
- Verifica che i canali di distribuzione siano stati impostati correttamente e, una volta confermati, verifica che la registrazione AWS Config sia corretta.

Per ulteriori informazioni, consulta il blog sulle best practice di AWS Config.

Registrazione e monitoraggio AWS Config

AWS Config è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un AWS servizio in AWS Config. Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS Config AWS soluzioni esistenti.

Argomenti

- Registrazione delle chiamate AWS Config API con AWS CloudTrail
- Monitoraggio

Registrazione delle chiamate AWS Config API con AWS CloudTrail

CloudTrail acquisisce tutte le chiamate API per AWS Config gli eventi as. Le chiamate acquisite includono chiamate dalla AWS Config console e chiamate di codice alle operazioni AWS Config API. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AWS Config Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviata AWS Config, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Argomenti

- AWS Config Informazioni in CloudTrail
- Comprensione delle AWS Config voci dei file di registro
- Esempio di file di log

AWS Config Informazioni in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in AWS Config, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare

eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuo sito Account AWS, inclusi gli eventi di AWS Config, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un trail
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte AWS Config le operazioni vengono registrate CloudTrail e documentate nell'AWS Config API Reference. Ad esempio, le chiamate alle operazioni DeliverConfigSnapshot, DeleteDeliveryChannel e DescribeDeliveryChannels generano voci nei file di registro. CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity.

Comprensione delle AWS Config voci dei file di registro

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni

sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Esempio di file di log

Per esempi di voci di CloudTrail registro, consultate i seguenti argomenti.

DeleteDeliveryChannel

Di seguito è riportato un file di CloudTrail registro di esempio per l'operazione DeleteDeliveryChannel.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DeliverConfigSnapshot

Di seguito è riportato un file di CloudTrail registro di esempio per l'operazione DeliverConfigSnapshot.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```

DescribeConfigurationRecorderStatus

Di seguito è riportato un file di CloudTrail registro di esempio per l'DescribeConfigurationRecorderStatusoperazione.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeConfigurationRecorders

Di seguito è riportato un file di CloudTrail registro di esempio per l'operazione DescribeConfigurationRecorders.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
```

```
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeDeliveryChannels

Di seguito è riportato un file di CloudTrail registro di esempio per l'operazione DescribeDeliveryChannels.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

GetResourceConfigHistory

Di seguito è riportato un file di CloudTrail registro di esempio per l'GetResourceConfigHistoryoperazione.


```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "GetResourceConfigHistory",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "limit": 0,
        "laterTime": "Dec 11, 2014 12:58:42 AM",
        "earlierTime": "Dec 10, 2014 4:58:42 PM"
      },
      "responseElements": null,
      "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
      "eventType": "AwsApiCall",
```

```
      "recipientAccountId": "111111111111"
      }
```

PutConfigurationRecorder

Di seguito è riportato un file di CloudTrail registro di esempio per l'operazione PutConfigurationRecorder.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:23Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorder": {
          "name": "default",
          "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
        }
      },
      "responseElements": null,
      "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

PutDeliveryChannel

Di seguito è riportato un file di CloudTrail registro di esempio per l'operazione PutDeliveryChannel.

```
{
```

```
        "eventVersion": "1.02",
        "userIdentity": {
          "type": "IAMUser",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::222222222222:user/JohnDoe",
          "accountId": "222222222222",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "userName": "JohnDoe"
        },
        "eventTime": "2014-12-11T18:33:08Z",
        "eventSource": "config.amazonaws.com",
        "eventName": "PutDeliveryChannel",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
        "requestParameters": {
          "deliveryChannel": {
            "name": "default",
            "s3BucketName": "config-api-test-pdx",
            "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
          }
        },
        "responseElements": null,
        "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
        "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
        "eventType": "AwsApiCall",
        "recipientAccountId": "222222222222"
      }
```

StartConfigurationRecorder

Di seguito è riportato un file di CloudTrail registro di esempio per l'operazione StartConfigurationRecorder.

```
{
        "eventVersion": "1.02",
        "userIdentity": {
          "type": "IAMUser",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::222222222222:user/JohnDoe",
          "accountId": "222222222222",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "userName": "JohnDoe"
```

```
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StopConfigurationRecorder

Di seguito è riportato un file di CloudTrail registro di esempio per l'operazione StopConfigurationRecorder.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
```

```
    "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
    "eventType": "AwsApiCall",
    "recipientAccountId": "222222222222"
  }
```

Monitoraggio

È possibile utilizzare altri AWS servizi per monitorare AWS Config le risorse.

- Puoi utilizzare Amazon Simple Notification Service (SNS) per inviarti notifiche ogni volta che una AWS risorsa supportata viene creata, aggiornata o modificata in altro modo a seguito dell'attività dell'API dell'utente.
- Puoi usare Amazon EventBridge per rilevare e reagire ai cambiamenti nello stato degli AWS Config eventi.

Argomenti

- Monitoraggio AWS delle modifiche alle risorse con Amazon SQS
- Monitoraggio AWS Config con Amazon EventBridge

Monitoraggio AWS delle modifiche alle risorse con Amazon SQS

AWS Config utilizza Amazon Simple Notification Service (SNS) per inviarti notifiche ogni volta che una AWS risorsa supportata viene creata, aggiornata o modificata in altro modo a seguito dell'attività dell'API dell'utente. Tuttavia, potresti essere interessato alle modifiche della configurazione relative solo a specifiche risorse. Ad esempio, potresti considerare fondamentale sapere quando viene modificata la configurazione di un gruppo di sicurezza, ma non ritieni necessario ricevere notifiche per ogni modifica ai tag delle istanze Amazon EC2. In alternativa, puoi scrivere un programma che esegue azioni specifiche quando risorse specifiche vengono aggiornate. Ad esempio, potresti voler avviare un determinato flusso di lavoro quando viene modificata la configurazione di un gruppo di sicurezza. Se desideri utilizzare programmaticamente i dati da AWS Config questi o altri modi, utilizza una coda di Amazon Simple Queue Service come endpoint di notifica per Amazon SNS.

> **Note**
>
> Le notifiche possono anche provenire da Amazon SNS sotto forma di e-mail, messaggio SMS (Short Message Service) verso cellulari e smartphone compatibili, messaggio di notifica verso

un'applicazione su un dispositivo mobile o messaggio di notifica a uno o più endpoint HTTP o HTTPS.

Puoi avere una singola coda SQS per sottoscrivere più argomenti, indipendentemente dal fatto che tu abbia un argomento per ogni regione o un argomento per ogni account per ogni regione. Devi sottoscrivere la coda all'argomento SNS desiderato. (Puoi sottoscrivere molteplici code a un unico argomento SNS). Per ulteriori informazioni, consulta Invio di messaggi Amazon SNS a code Amazon SQS.

Autorizzazioni per Amazon SQS

Per utilizzare Amazon SQS con AWS Config, devi configurare una policy che conceda al tuo account le autorizzazioni per eseguire tutte le azioni consentite su una coda SQS. La policy di esempio seguente concede all'account numero 111122223333 e all'account numero 444455556666 l'autorizzazione all'invio di messaggi relativi a ogni modifica della configurazione verso la coda denominata arn:aws:sqs:us-east-2:444455556666:queue1.

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
}
```

Inoltre, è necessario creare una policy che conceda le autorizzazioni alle connessioni tra un argomento SNS e la coda SQS che si sottoscrive a tale argomento. Di seguito è riportato un esempio di policy che consente all'argomento SNS con Amazon Resource Name (ARN) arn:aws:sns:us-east-2:111122223333:test-topic di eseguire qualsiasi azione sulla coda denominata arn:aws:sqs:us-east-2:111122223333:. test-topic-queue

> **Note**
>
> Gli account dell'argomento SNS e della coda SQS devono appartenere alla stessa regione.

```
{
  "Version": "2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

Ogni policy può includere istruzioni che riguardano solo una singola coda, non più code. Per informazioni su altre restrizioni sulle policy di Amazon SQS, consulta Informazioni specifiche alle policy Amazon SQS.

Monitoraggio AWS Config con Amazon EventBridge

Amazon EventBridge offre un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle AWS risorse. Usa Amazon EventBridge per rilevare e reagire ai cambiamenti nello stato degli AWS Config eventi.

Puoi scegliere di creare una regola che venga eseguita ogni volta che si verifica una transizione di stato o quando si verifica una transizione verso uno o più stati di interesse. Quindi, in base alle regole che EventBridge crei, Amazon richiama una o più azioni mirate quando un evento corrisponde ai valori specificati in una regola. A seconda del tipo di evento, potresti voler inviare notifiche, acquisire informazioni sull'evento, intraprendere un'azione correttiva, avviare eventi o eseguire altre operazioni.

Prima di creare regole per gli eventi AWS Config, tuttavia, devi fare quanto segue:

- Acquisisci familiarità con eventi, regole e obiettivi in. EventBridge Per ulteriori informazioni, consulta What Is Amazon EventBridge?
- Per ulteriori informazioni su come iniziare EventBridge e configurare le regole, consulta la pagina Guida introduttiva ad Amazon EventBridge.
- Crea la destinazione o le destinazioni da utilizzare nelle regole degli eventi.

Argomenti

- EventBridge Formato Amazon per AWS Config
- Creazione di Amazon EventBridge Rule per AWS Config

EventBridge Formato Amazon per AWS Config

L' EventBridge evento per AWS Config ha il seguente formato:

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "event type",
   "source": "aws.config",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [
      resources
   ],
   "detail": {
      specific message type
   }
}
```

Creazione di Amazon EventBridge Rule per AWS Config

Utilizza i seguenti passaggi per creare una EventBridge regola che si attiva in base a un evento emesso da. AWS Config Gli eventi vengono emessi secondo il principio del massimo sforzo.

1. Nel pannello di navigazione, scegli Regole.
2. Scegli Create rule (Crea regola).
3. Inserire un nome e una descrizione per la regola.

   Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso router di eventi.
4. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
5. Per Origine dell'evento, scegli AWS eventi o eventi EventBridge partner.
6. (Opzionale) In Tipo evento di esempio, seleziona Eventi AWS .
7. (Opzionale) In Eventi di esempio, seleziona il tipo di evento che deve attivare la regola:
   - Scegli AWS API Call via CloudTrail per basare le regole sulle chiamate API effettuate a questo servizio. Per ulteriori informazioni sulla creazione di questo tipo di regola, consulta Tutorial: Crea una EventBridge regola Amazon per le chiamate AWS CloudTrail API.
   - Scegli Config Configuration Item Change (Modifica all'elemento della configurazione di Config) per ricevere una notifica quando una risorsa nel tuo account subisce modifiche.

     Come descritto in questi articoli di supporto, puoi utilizzare EventBridge per ricevere notifiche e-mail personalizzate quando una risorsa viene creata o eliminata. Come posso ricevere notifiche e-mail personalizzate quando una risorsa viene creata nel mio AWS Config servizio di Account AWS utilizzo? e come posso ricevere notifiche e-mail personalizzate quando una risorsa viene eliminata nel mio AWS Config servizio di Account AWS utilizzo? .
   - Scegli Config Rules Compliance Change (Modifica alla conformità delle regole di Config) per ricevere una notifica quando un controllo di conformità delle regole ha esito negativo.

     Come descritto in questo articolo di supporto, è possibile utilizzare EventBridge per ricevere notifiche e-mail personalizzate quando una risorsa non è conforme. Come posso ricevere una notifica quando una AWS risorsa non è conforme utilizzando? AWS Config.
   - Scegli Config Rules Re-evaluation Status (Stato rivalutazione delle regole di Config) per ricevere una notifica sullo stato della rivalutazione.
   - Scegli Config Configuration Snapshot Delivery Status (Stato distribuzione snapshot di configurazione di Config) per ricevere una notifica sullo stato di distribuzione degli snapshot di configurazione.
   - Scegli Config Configuration Snapshot Delivery Status (Stato distribuzione cronologia di configurazione di Config) per ricevere una notifica sullo stato di distribuzione della cronologia di configurazione.

8. In Metodo di creazione scegli Utilizza modulo del modello.
9. Per Origine evento, scegli Servizi AWS .
10. In Servizio AWS , scegli Config.
11. In Tipo di evento, seleziona il tipo di evento che deve attivare la regola:
    - Scegli Tutti gli eventi per creare una regola che si applichi a tutti i AWS servizi. Se selezioni questa opzione, non puoi scegliere tipi di messaggi specifici, nomi di regole, tipi di risorse o ID delle risorse.
    - Scegli AWS API Call via CloudTrail per basare le regole sulle chiamate API effettuate a questo servizio. Per ulteriori informazioni sulla creazione di questo tipo di regola, consulta Tutorial: Crea una EventBridge regola Amazon per le chiamate AWS CloudTrail API.
    - Scegli Config Configuration Item Change (Modifica all'elemento della configurazione di Config) per ricevere una notifica quando una risorsa nel tuo account subisce modifiche.

      Come descritto in questi articoli di supporto, puoi utilizzare EventBridge per ricevere notifiche e-mail personalizzate quando una risorsa viene creata o eliminata. Come posso ricevere notifiche e-mail personalizzate quando una risorsa viene creata nel mio AWS Config servizio di Account AWS utilizzo? e come posso ricevere notifiche e-mail personalizzate quando una risorsa viene eliminata nel mio AWS Config servizio di Account AWS utilizzo? .
    - Scegli Config Rules Compliance Change (Modifica alla conformità delle regole di Config) per ricevere una notifica quando un controllo di conformità delle regole ha esito negativo.

      Come descritto in questo articolo di supporto, è possibile utilizzare EventBridge per ricevere notifiche e-mail personalizzate quando una risorsa non è conforme. Come posso ricevere una notifica quando una AWS risorsa non è conforme utilizzando? AWS Config.
    - Scegli Config Rules Re-evaluation Status (Stato rivalutazione delle regole di Config) per ricevere una notifica sullo stato della rivalutazione.
    - Scegli Config Configuration Snapshot Delivery Status (Stato distribuzione snapshot di configurazione di Config) per ricevere una notifica sullo stato di distribuzione degli snapshot di configurazione.
    - Scegli Config Configuration Snapshot Delivery Status (Stato distribuzione cronologia di configurazione di Config) per ricevere una notifica sullo stato di distribuzione della cronologia di configurazione.
12. Scegli Any message type (Qualsiasi tipo di messaggio) per ricevere notifiche di qualsiasi tipo. Scegli Specific message type(s) (Tipo/i di messaggio specifico/i) per ricevere i seguenti tipi di notifiche:

- Se lo scegli ConfigurationItemChangeNotification, ricevi messaggi quando la configurazione di una risorsa che AWS Config valuta è cambiata.
- Se scegli ComplianceChangeNotifica, ricevi messaggi quando il tipo di conformità di una risorsa che AWS Config valuta è cambiato.
- Se si sceglie questa opzione ConfigRulesEvaluationStarted, si ricevono messaggi quando si AWS Config inizia a valutare la regola rispetto alle risorse specificate.
- Se lo desideri ConfigurationSnapshotDeliveryCompleted, riceverai messaggi quando consegnerai AWS Config correttamente lo snapshot di configurazione al tuo bucket Amazon S3.
- Se lo desideri ConfigurationSnapshotDeliveryFailed, ricevi messaggi quando AWS Config non riesci a consegnare lo snapshot di configurazione al tuo bucket Amazon S3.
- Se lo desideri ConfigurationSnapshotDeliveryStarted, riceverai messaggi quando AWS Config inizia a distribuire lo snapshot di configurazione al tuo bucket Amazon S3.
- Se lo desideri ConfigurationHistoryDeliveryCompleted, riceverai messaggi quando invii AWS Config correttamente la cronologia di configurazione al tuo bucket Amazon S3.

13. Se hai scelto un tipo di evento specifico dall'elenco a discesa Tipo di evento, scegli Qualsiasi tipo di risorsa per creare una regola che si applichi a tutti i tipi di risorse AWS Config supportati.

    Oppure scegli Specific resource type(s) (Tipo/i specifico/i di risorse), quindi digita il tipo di risorsa di AWS Config supportato (ad esempio `AWS::EC2::Instance`).

14. Se scegli uno specifico tipo di evento dall'elenco a discesa Tipo di evento, scegli Qualsiasi ID di risorsa per includere tutti gli ID di risorsa AWS Config supportati.

    Oppure scegli Specific resource ID(s) (ID specifico/i di risorse), quindi digita l'ID della risorsa di AWS Config supportata (ad esempio `i-04606de676e635647`).

15. Se scegli uno specifico tipo di evento dall'elenco a discesa Tipo di evento, scegli Qualsiasi nome di regola per includere tutti le regole AWS Config supportate.

    Oppure scegli Specific resource type(s) (Tipo/i specifico/i di risorse), quindi digita la regola di AWS Config supportata (ad esempio required-tags).

16. In Seleziona destinazioni, scegli il tipo di destinazione da utilizzare con questa regola, quindi configura le eventuali altre opzioni richieste da questo tipo specifico.

17. I campi visualizzati variano a seconda del servizio scelto. Se necessario, inserisci le informazioni specifiche per questo tipo di destinazione.

18. Per molti tipi di oggetto, EventBridge sono necessarie le autorizzazioni per inviare eventi alla destinazione. In questi casi, EventBridge può creare il ruolo IAM necessario per l'esecuzione della regola.
    - Per creare un ruolo IAM automaticamente, seleziona Crea un nuovo ruolo per questa risorsa specifica.
    - Per utilizzare un ruolo IAM creato in precedenza, seleziona Use existing role (Utilizza un ruolo esistente).
19. (Facoltativo) Scegliere Add target (Aggiungi target) per aggiungere un altro target per questa regola.
20. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta Amazon EventBridge tags.
21. Verifica la configurazione delle regole per accertarti che soddisfi i tuoi requisiti di monitoraggio di eventi.
22. Scegli Crea per confermare la scelta.

Utilizzo AWS Config con l'interfaccia Amazon VPC Endpoints

Se utilizzi Amazon Virtual Private Cloud (Amazon VPC) per ospitare AWS le tue risorse, puoi stabilire una connessione privata tra il tuo VPC e. AWS ConfigÈ possibile utilizzare questa connessione per comunicare con AWS Config dal VPC senza accedere all'Internet pubblico.

Amazon VPC è un AWS servizio che puoi utilizzare per avviare AWS risorse in una rete virtuale definita dall'utente. Con un VPC;, detieni il controllo delle impostazioni della rete, come l'intervallo di indirizzi IP, le sottoreti, le tabelle di routing e i gateway di rete. Gli endpoint VPC di interfaccia sono alimentati da AWS PrivateLink, una AWS tecnologia che consente la comunicazione privata tra AWS i servizi utilizzando un'interfaccia di rete elastica con indirizzi IP privati. Per connettere il tuo VPC AWS Config, definisci un'interfaccia VPC endpoint per. AWS Config Questo tipo di endpoint ti consente di connettere il tuo VPC AWS ai servizi. L'endpoint fornisce una connettività affidabile e scalabile AWS Config senza richiedere un gateway Internet, un'istanza NAT (Network Address Translation) o una connessione VPN. Per ulteriori informazioni, consulta Che cos'è Amazon VPC? nella Guida per l'utente di Amazon VPC.

Le fasi seguenti sono per gli utenti Amazon VPC. Per ulteriori informazioni, consulta l'argomento relativo alle nozioni di base nella Guida per l'utente di Amazon VPC.

Crea un endpoint VPC per AWS Config

Per iniziare a utilizzarlo AWS Config con il tuo VPC, crea un endpoint VPC di interfaccia per. AWS Config Non è necessario modificare le impostazioni per. AWS Config AWS Config chiama altri AWS servizi utilizzando i relativi endpoint pubblici. Per ulteriori informazioni, consulta Creazione di un endpoint di interfaccia nella Guida per l'utente di Amazon VPC.

Domande frequenti

Non riesco a vedere le mie ultime modifiche alla configurazione

Posso aspettarmi di vedere subito le mie modifiche alla configurazione?

AWS Config di solito registra le modifiche alla configurazione delle risorse subito dopo che viene rilevata una modifica o alla frequenza specificata. Tuttavia, questa operazione viene effettuata con il massimo impegno e a volte può richiedere più tempo. Se i problemi persistono dopo qualche tempo, contatta AWS Supporte fornisci le tue AWS Config metriche supportate da Amazon. CloudWatch Per informazioni su queste metriche, consulta Metriche di AWS Config utilizzo e successo.

Relazioni indirette in AWS Config

Argomenti

- Cos'è la relazione tra risorse?
- Che cos'è una relazione diretta e indiretta rispetto a una risorsa?
- Quali relazioni indirette supporta AWS Config ?
- Come vengono creati gli elementi di configurazione come conseguenza delle relazioni dirette e indirette?
- Quali sono gli elementi di configurazione generati n base alle relazioni indirette?
- Come posso recuperare i dati di configurazione relativi alle relazioni indirette?

Cos'è la relazione tra risorse?

Nel AWS, le risorse si riferiscono a entità gestibili, come un'istanza Amazon Elastic Compute Cloud (Amazon EC2) AWS CloudFormation , uno stack o un bucket Amazon S3. AWS Config è un servizio che traccia e monitora le risorse creando elementi di configurazione (CI) ogni volta che viene rilevata una modifica a un tipo di risorsa registrata o alla frequenza di registrazione impostata. Ad esempio, quando AWS Config è configurato per tracciare le istanze Amazon EC2, crea un elemento di configurazione ogni volta che un'istanza viene creata, aggiornata o eliminata. Ogni elemento di configurazione creato da AWS Config ha diversi campi`accountId`, tra cui `arn` (Amazon Resource Name) `awsRegionconfiguration`,`tags`, `erelationships`. Il campo delle relazioni di un CI consente di AWS Config visualizzare in che modo le risorse sono collegate tra loro. Ad esempio, una

relazione può indicare che un volume Amazon EBS con ID `vol-123ab45d` è collegato a un'istanza Amazon EC2 con ID `i-a1b2c3d4`, associata al gruppo di sicurezza `sg-ef678hk`.

Che cos'è una relazione diretta e indiretta rispetto a una risorsa?

AWS Config ricava le relazioni per la maggior parte dei tipi di risorse dal campo di configurazione, chiamate relazioni «dirette». Una relazione diretta è una connessione unidirezionale (A→B) tra una risorsa (A) e un'altra risorsa (B), in genere ottenuta dalla risposta API di descrizione della risorsa (A). In passato, per alcuni tipi di risorse AWS Config inizialmente supportati, acquisiva anche le relazioni derivanti dalle configurazioni di altre risorse, creando relazioni «indirette» bidirezionali (B→A). Ad esempio, la relazione tra un'istanza Amazon EC2 e il relativo gruppo di sicurezza è diretta perché i gruppi di sicurezza sono inclusi nella risposta API di descrizione per l'istanza Amazon EC2. Al contrario, la relazione tra un gruppo di sicurezza e un'istanza Amazon EC2 è indiretta perché la descrizione di un gruppo di sicurezza non restituisce alcuna informazione sulle istanze a cui è associato. Di conseguenza, quando viene rilevata una modifica alla configurazione di una risorsa, AWS Config non solo crea un elemento di configurazione per quella risorsa, ma genera anche gli elementi di configurazione per tutte le risorse correlate, comprese quelle con relazioni indirette. Ad esempio, quando AWS Config rileva modifiche in un'istanza Amazon EC2, crea un CI per l'istanza e un CI per il gruppo di sicurezza associato all'istanza.

Quali relazioni indirette supporta AWS Config ?

Sono supportate le seguenti relazioni indirette con le risorse AWS Config.

Tipo di risorsa	relazione indiretta con il tipo di risorsa		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface` , `AWS::EC2::Subnet` , `AWS::EC2::VPNGateway` , `AWS::EC2::VPC`		

Tipo di risorsa	relazione indiretta con il tipo di risorsa		
AWS::EC2::EIP	AWS::EC2::Instance , AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway , AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		

Tipo di risorsa	relazione indiretta con il tipo di risorsa		
`AWS::EC2::Subnet`	`AWS::EC2::VPC`		
`AWS::EC2::VPNGateway`	`AWS::EC2::VPC`		

Come vengono creati gli elementi di configurazione come conseguenza delle relazioni dirette e indirette?

Per una relazione diretta tra risorse (A→B), qualsiasi modifica alla configurazione della risorsa B avvierà un elemento di configurazione anche per la risorsa A. Analogamente, per una relazione indiretta (B→A), in caso di modifica alla configurazione della risorsa A, verrà generato un nuovo elemento di configurazione per la risorsa B. Ad esempio, tra un'istanza Amazon EC2 e un gruppo di sicurezza c'è una relazione diretta, quindi qualsiasi modifica alla configurazione di un gruppo di sicurezza genera un elemento di configurazione per il gruppo di sicurezza e un elemento di configurazione per l'istanza EC2. Allo stesso modo, tra il gruppo di sicurezza e l'istanza Amazon EC2 c'è una relazione indiretta, quindi qualsiasi modifica alla configurazione di un'istanza EC2 genera un elemento di configurazione per l'istanza Amazon EC2 e un elemento di configurazione per il gruppo di sicurezza.

Quali sono gli elementi di configurazione generati n base alle relazioni indirette?

Di seguito sono riportati gli elementi di configurazione aggiuntivi generati come conseguenza delle relazioni indirette tra le risorse.

Modifiche alla configurazione dei seguenti tipi di risorse	genera elementi di configurazione per i seguenti tipi di risorse		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance`, `AWS::EC2:`		

Modifiche alla configurazione dei seguenti tipi di risorse	genera elementi di configurazione per i seguenti tipi di risorse		
	:NetworkInterface , AWS::EC2::Subnet , AWS::EC2::VPNGateway , e AWS::EC2::VPC		
AWS::EC2::EIP	AWS::EC2::Instance , AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		

Modifiche alla configurazione dei seguenti tipi di risorse	genera elementi di configurazione per i seguenti tipi di risorse		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway , AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

Come posso recuperare i dati di configurazione relativi alle relazioni indirette?

È possibile eseguire query SQL (Structured Query Language) in AWS Config Advanced Queries per recuperare i dati di configurazione relativi alle relazioni indirette tra le risorse. Ad esempio, se desideri recuperare l'elenco delle istanze Amazon EC2 relative a un gruppo di sicurezza, utilizza la seguente query:

```
SELECT
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
    AND
```

```
    relationships.resourceId = 'sg-234213'
```

Esempi di codice per l' AWS Config utilizzo degli AWS SDK

I seguenti esempi di codice mostrano come utilizzarlo AWS Config con un kit di sviluppo AWS software (SDK).

Le operazioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le operazioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati e negli esempi tra servizi.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice

- Azioni per l' AWS Config utilizzo AWS degli SDK
  - Utilizzo DeleteConfigRule con un AWS SDK o una CLI
  - Utilizzo DescribeComplianceByConfigRule con un AWS SDK o una CLI
  - Utilizzo DescribeComplianceByResource con un AWS SDK o una CLI
  - Utilizzo DescribeConfigRuleEvaluationStatus con un AWS SDK o una CLI
  - Utilizzo DescribeConfigRules con un AWS SDK o una CLI
  - Utilizzo DescribeConfigurationRecorderStatus con un AWS SDK o una CLI
  - Utilizzo DescribeConfigurationRecorders con un AWS SDK o una CLI
  - Utilizzo DescribeDeliveryChannels con un AWS SDK o una CLI
  - Utilizzo GetComplianceDetailsByConfigRule con un AWS SDK o una CLI
  - Utilizzo GetComplianceDetailsByResource con un AWS SDK o una CLI
  - Utilizzo GetComplianceSummaryByConfigRule con un AWS SDK o una CLI
  - Utilizzo GetComplianceSummaryByResourceType con un AWS SDK o una CLI
  - Utilizzo PutConfigRule con un AWS SDK o una CLI
  - Utilizzo PutDeliveryChannel con un AWS SDK o una CLI

Azioni per l' AWS Config utilizzo AWS degli SDK

I seguenti esempi di codice mostrano come eseguire AWS Config azioni individuali con gli AWS SDK. Questi estratti richiamano l' AWS Config API e sono estratti di codice di programmi più grandi

che devono essere eseguiti nel contesto. Ogni esempio include un collegamento a GitHub, dove è possibile trovare le istruzioni per la configurazione e l'esecuzione del codice.

Gli esempi seguenti includono solo le operazioni più comunemente utilizzate. Per un elenco completo, consulta la Documentazione di riferimento delle API AWS Config.

Esempi

- Utilizzo DeleteConfigRule con un AWS SDK o una CLI
- Utilizzo DescribeComplianceByConfigRule con un AWS SDK o una CLI
- Utilizzo DescribeComplianceByResource con un AWS SDK o una CLI
- Utilizzo DescribeConfigRuleEvaluationStatus con un AWS SDK o una CLI
- Utilizzo DescribeConfigRules con un AWS SDK o una CLI
- Utilizzo DescribeConfigurationRecorderStatus con un AWS SDK o una CLI
- Utilizzo DescribeConfigurationRecorders con un AWS SDK o una CLI
- Utilizzo DescribeDeliveryChannels con un AWS SDK o una CLI
- Utilizzo GetComplianceDetailsByConfigRule con un AWS SDK o una CLI
- Utilizzo GetComplianceDetailsByResource con un AWS SDK o una CLI
- Utilizzo GetComplianceSummaryByConfigRule con un AWS SDK o una CLI
- Utilizzo GetComplianceSummaryByResourceType con un AWS SDK o una CLI
- Utilizzo PutConfigRule con un AWS SDK o una CLI
- Utilizzo PutDeliveryChannel con un AWS SDK o una CLI

Utilizzo **`DeleteConfigRule`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DeleteConfigRule`.

CLI

AWS CLI

Per eliminare una regola di AWS Config

Il comando seguente elimina una regola AWS Config denominata: `MyConfigRule`

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Per i dettagli sull'API, vedere DeleteConfigRulein AWS CLI Command Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- Per i dettagli sull'API, consulta DeleteConfigRule AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeComplianceByConfigRule`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeComplianceByConfigRule`.

CLI

AWS CLI

Per ottenere informazioni sulla conformità per le regole di AWS Config

Il comando seguente restituisce informazioni sulla conformità per ogni regola di AWS Config violata da una o più risorse: AWS

```
aws configservice describe-compliance-by-config-rule --compliance-types
 NON_COMPLIANT
```

Nell'output, il valore di ogni `CappedCount` attributo indica quante risorse non sono conformi alla regola correlata. Ad esempio, l'output seguente indica che 3 risorse non sono conformi alla regola denominata`InstanceTypesAreT2micro`.

Output:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
```

```
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Per i dettagli sull'API, consulta DescribeComplianceByConfigRule AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio recupera i dettagli di conformità per la regola ebs-optimized-instance, per la quale non esistono risultati di valutazione correnti per la regola, quindi restituisce INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Output:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Esempio 2: questo esempio restituisce il numero di risorse non conformi per la regola ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Per i DescribeComplianceByConfigRuledettagli AWS Tools for PowerShell sull'API, vedere in Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeComplianceByResource`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeComplianceByResource`.

CLI

AWS CLI

Per ottenere informazioni sulla conformità delle tue risorse AWS

Il comando seguente restituisce informazioni sulla conformità per ogni istanza EC2 registrata da AWS Config e che viola una o più regole:

```
aws configservice describe-compliance-by-resource --resource-type
 AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

Nell'output, il valore di ogni `CappedCount` attributo indica quante regole la risorsa viola. Ad esempio, l'output seguente indica che l'istanza `i-1a2b3c4d` viola 2 regole.

Output:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
```

```
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- Per i dettagli sull'API, consulta DescribeComplianceByResource AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio verifica il tipo di **`AWS::SSM::ManagedInstanceInventory`** risorsa per il tipo di conformità «COMPLIANT».

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Output:

```
Compliance                            ResourceId          ResourceType
----------                            ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Per i dettagli sull'API, vedere DescribeComplianceByResourcein AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeConfigRuleEvaluationStatus`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeConfigRuleEvaluationStatus`.

CLI

AWS CLI

Per ottenere informazioni sullo stato di una regola di AWS Config

Il comando seguente restituisce le informazioni sullo stato di una regola AWS Config denominata: `MyConfigRule`

```
aws configservice describe-config-rule-evaluation-status --config-rule-names
 MyConfigRule
```

Output:

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- Per i dettagli sull'API, vedere DescribeConfigRuleEvaluationStatusin AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio restituisce le informazioni sullo stato delle regole di configurazione specificate.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

Output:

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- Per i dettagli sull'API, vedere DescribeConfigRuleEvaluationStatusin AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeConfigRules`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeConfigRules`.

CLI

AWS CLI

Per ottenere dettagli su una regola di AWS Config

Il comando seguente restituisce i dettagli per una regola AWS Config denominata: `InstanceTypesAreT2micro`

```
aws configservice describe-config-rules --config-rule-names
 InstanceTypesAreT2micro
```

Output:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
```

```
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- Per i dettagli sull'API, vedere DescribeConfigRulesin AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio elenca le regole di configurazione per l'account, con le proprietà selezionate.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Output:

```
ConfigRuleName                                      ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                      ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                               config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                 config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required          config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Per i dettagli sull'API, vedere DescribeConfigRulesin AWS Tools for PowerShell Cmdlet Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- Per i dettagli sull'API, consulta DescribeConfigRules AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeConfigurationRecorderStatus`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeConfigurationRecorderStatus`.

CLI

AWS CLI

Per ottenere informazioni sullo stato del registratore di configurazione

Il comando seguente restituisce lo stato del registratore di configurazione predefinito:

```
aws configservice describe-configuration-recorder-status
```

Output:

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- Per i dettagli sull'API, consulta DescribeConfigurationRecorderStatus AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: Questo esempio restituisce lo stato dei registratori di configurazione.

```
Get-CFGConfigurationRecorderStatus
```

Output:

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- Per i dettagli sull'API, vedere DescribeConfigurationRecorderStatusin AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeConfigurationRecorders`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeConfigurationRecorders`.

CLI

AWS CLI

Per ottenere dettagli sul registratore di configurazione

Il comando seguente restituisce dettagli sul registratore di configurazione predefinito:

```
aws configservice describe-configuration-recorders
```

Output:

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- Per i dettagli sull'API, consultate DescribeConfigurationRecorders AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: Questo esempio restituisce i dettagli dei registratori di configurazione.

```
Get-CFGConfigurationRecorder | Format-List
```

Output:

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- Per i dettagli sull'API, vedere DescribeConfigurationRecordersin AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`DescribeDeliveryChannels`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`DescribeDeliveryChannels`.

CLI

AWS CLI

Per ottenere dettagli sul canale di distribuzione

Il comando seguente restituisce i dettagli sul canale di consegna:

```
aws configservice describe-delivery-channels
```

Output:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- Per i dettagli sull'API, consulta DescribeDeliveryChannels AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio recupera il canale di consegna per la regione e visualizza i dettagli.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Output:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Per i dettagli sull'API, vedere DescribeDeliveryChannelsin AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetComplianceDetailsByConfigRule`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`GetComplianceDetailsByConfigRule`.

CLI

AWS CLI

Per ottenere i risultati della valutazione per una regola AWS Config

Il comando seguente restituisce i risultati della valutazione per tutte le risorse che non sono conformi a una regola AWS Config denominata: `InstanceTypesAreT2micro`

```
aws configservice get-compliance-details-by-config-rule --config-rule-name
 InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
```

```
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Per i dettagli sull'API, consulta GetComplianceDetailsByConfigRule AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio ottiene i risultati della valutazione per la regola access-keys-rotated e restituisce l'output raggruppato per tipo di conformità

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Output:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Esempio 2: questo esempio richiede i dettagli di conformità per la regola per le risorse COMPLIANT. access-keys-rotated

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Output:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Per i dettagli sull'API, vedere GetComplianceDetailsByConfigRulein AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetComplianceDetailsByResource`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`GetComplianceDetailsByResource`.

CLI

AWS CLI

Per ottenere i risultati della valutazione di una risorsa AWS

Il comando seguente restituisce i risultati della valutazione per ogni regola a cui l'istanza EC2 `i-1a2b3c4d` non è conforme:

```
aws configservice get-compliance-details-by-resource --resource-type
 AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
```

```
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Per i dettagli sull'API, consulta GetComplianceDetailsByResource AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: Questo esempio di risultati di valutazione per la risorsa data.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Output:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- Per i dettagli sull'API, vedere GetComplianceDetailsByResourcein AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetComplianceSummaryByConfigRule`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`GetComplianceSummaryByConfigRule`.

CLI

AWS CLI

Per ottenere il riepilogo della conformità per le tue regole di AWS Config

Il comando seguente restituisce il numero di regole conformi e il numero di regole non conformi:

```
aws configservice get-compliance-summary-by-config-rule
```

Nell'output, il valore di ogni `CappedCount` attributo indica quante regole sono conformi o non conformi.

Output:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- Per i dettagli sull'API, consulta Command Reference. GetComplianceSummaryByConfigRuleAWS CLI

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio restituisce il numero di regole di Config non conformi.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Per i dettagli sull'API, vedere GetComplianceSummaryByConfigRulein Cmdlet Reference.AWS Tools for PowerShell

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetComplianceSummaryByResourceType`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`GetComplianceSummaryByResourceType`.

CLI

AWS CLI

Per ottenere il riepilogo della conformità per tutti i tipi di risorse

Il comando seguente restituisce il numero di AWS risorse non conformi e il numero di risorse conformi:

```
aws configservice get-compliance-summary-by-resource-type
```

Nell'output, il valore di ogni `CappedCount` attributo indica quante risorse sono conformi o non conformi.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

Per ottenere il riepilogo della conformità per un tipo di risorsa specifico

Il comando seguente restituisce il numero di istanze EC2 non conformi e il numero di istanze conformi:

```
aws configservice get-compliance-summary-by-resource-type --resource-types
 AWS::EC2::Instance
```

Nell'output, il valore di ogni `CappedCount` attributo indica quante risorse sono conformi o non conformi.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
```

```
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- Per i dettagli sull'API, consulta Command Reference. GetComplianceSummaryByResourceTypeAWS CLI

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio restituisce il numero di risorse conformi o non conformi e converte l'output in json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Per i dettagli sull'API, vedere in Cmdlet Reference. GetComplianceSummaryByResourceTypeAWS Tools for PowerShell

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **PutConfigRule** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`PutConfigRule`.

CLI

AWS CLI

Per aggiungere una regola AWS Config gestita

Il comando seguente fornisce codice JSON per aggiungere una regola Config AWS gestita:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json`è un file JSON che contiene la configurazione delle regole:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Per l'`ComplianceResourceTypes`attributo, questo codice JSON limita l'ambito alle risorse del `AWS::EC2::Instance` tipo, quindi AWS Config valuterà solo le istanze EC2 rispetto alla regola. Poiché la regola è una regola gestita, l'`Owner`attributo è impostato su e l'`SourceIdentifier`attributo è impostato sull'identificatore della regola`AWS`,. `REQUIRED_TAGS` Per l'`InputParameters`attributo, vengono specificate le chiavi di tag richieste dalla regola `CostCenter` e`Owner`.

Se il comando ha esito positivo, AWS Config non restituisce alcun output. Per verificare la configurazione della regola, esegui il describe-config-rules comando e specifica il nome della regola.

Per aggiungere una regola Config gestita dal cliente

Il comando seguente fornisce il codice JSON per aggiungere una regola Config gestita dal cliente:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.jsonè` un file JSON che contiene la configurazione delle regole:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Per l'`ComplianceResourceTypes`attributo, questo codice JSON limita l'ambito alle risorse del `AWS::EC2::Instance` tipo, quindi AWS Config valuterà solo le istanze EC2 rispetto alla regola. Poiché questa regola è una regola gestita dal cliente, l'`Owner`attributo è impostato su e l'`SourceIdentifier`attributo è impostato sull'ARN della funzione Lambda AWS .

`CUSTOM_LAMBDA` L'`SourceDetails`oggetto è obbligatorio. I parametri specificati per l'`InputParameters`attributo vengono passati alla funzione AWS Lambda quando AWS Config la richiama per valutare le risorse rispetto alla regola.

Se il comando ha esito positivo, AWS Config non restituisce alcun output. Per verificare la configurazione della regola, esegui il describe-config-rules comando e specifica il nome della regola.

- Per i dettagli sull'API, consulta PutConfigRule AWS CLICommand Reference.

Python

SDK per Python (Boto3)

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
```

```
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Per i dettagli sull'API, consulta PutConfigRule AWSSDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`PutDeliveryChannel`** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare`PutDeliveryChannel`.

CLI

AWS CLI

Per creare un canale di distribuzione

Il comando seguente fornisce le impostazioni per il canale di consegna come codice JSON:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

Il `deliveryChannel.json` file specifica gli attributi del canale di consegna:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

L'esempio seguente imposta i seguenti attributi:

`name`- Il nome del canale di consegna. Per impostazione predefinita, AWS Config assegna il nome `default` a un nuovo canale di consegna. Non è possibile aggiornare il nome del canale di consegna con il comando. `put-delivery-channel` Per i passaggi per modificare il nome, consulta Ridenominazione del canale di consegna. `s3BucketName` - Il nome del bucket Amazon S3 a cui AWS Config fornisce istantanee di configurazione e file di cronologia della configurazione. Se si specifica un bucket che appartiene a un altro AWS account, tale bucket deve disporre di politiche che concedano le autorizzazioni di accesso a Config. AWS Per ulteriori informazioni, consulta Autorizzazioni per il bucket Amazon S3.

`snsTopicARN`- L'Amazon Resource Name (ARN) dell'argomento Amazon SNS a cui AWS Config invia notifiche sulle modifiche alla configurazione. Se scegli un argomento da un altro account, l'argomento deve avere politiche che concedano le autorizzazioni di accesso a Config. AWS Per ulteriori informazioni, consulta l'argomento Autorizzazioni per l'argomento Amazon SNS.

`configSnapshotDeliveryProperties`- Contiene l'`deliveryFrequency`attributo, che imposta la frequenza con cui AWS Config fornisce istantanee di configurazione e la frequenza con cui richiama le valutazioni per le regole di Config periodiche.

Se il comando ha esito positivo, AWS Config non restituisce alcun output. Per verificare le impostazioni del tuo canale di consegna, esegui il describe-delivery-channels comando.

- Per i dettagli sull'API, consulta PutDeliveryChannel AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio modifica la proprietà DeliveryFrequency di un canale di consegna esistente.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- Per i dettagli sull'API, vedere PutDeliveryChannelin AWS Tools for PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo AWS Config con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti alla documentazione per. AWS Config Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi abbonarti a un feed RSS.

- Versione API: 12-11-2014
- Ultimo aggiornamento della documentazione: 17 giugno 2024

Modifica	Descrizione	Data
Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Elastic File System (Amazon EFS), Amazon AWS Systems Manager per SAP Redshift e. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	17 giugno 2024
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • cloudtrail-s3-bucket-public-access proibito • registrazione degli accessi a cloudtrail-s3-bucket	8 maggio 2024
AWS Config aggiorna le regole gestite	Con questa versione, AWS Config supporta la seguente regola gestita: iam-external-access-analyzer-enabled	2 maggio 2024

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • guardduty è abilitato alla protezione da malware • abilitato alla protezione guardduty-rds • abilitato alla protezione guardduty-s3 • abilitato alla scansione standard di inspector-lambda	26 aprile 2024
AWS Config semplifica l'analisi dell'utilizzo con Amazon CloudWatch	Con questa versione, le CloudWatch metriche di Amazon per il monitoraggio dell'utilizzo AWS Config dei dati mostreranno solo l'utilizz o fatturabile. Ciò significa che l'utilizzo non fatturabile non verrà più visualizzato nelle CloudWatch metriche Amazon emesse e nella console. AWS Config AWS Config Ciò consente di convalida re la AWS Config configura zione e l'utilizzo utilizzando i CloudWatch parametri di Amazon e di correlare l'utilizzo fatturabile con i costi associati . Per ulteriori informazioni, consulta AWS Config Usage and Success Metrics.	26 aprile 2024

AWS Config aggiorna le regole gestite	Con questa versione, AWS Config supporta la seguente regola gestita: iam-server-certificate-expiration-check	23 aprile 2024
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • vpc-sg-port-restriction-check • cloudtrail-all-write-s3-data-event-check • cloudtrail-all-read-s3-data-event-check	17 aprile 2024
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • guardduty-eks-protection-audit-enabled • abilitato a guardduty-eks-protection-runtime • abilitato alla protezione lambda guardduty-lambda • abilitato a inspector-ec2-scan • abilitato a inspector-ecr-scan • abilitato a inspector-lambda-code-scan-scan • redshift - accesso illimitato alle porte	16 aprile 2024

AWS Config aggiorna le regole gestite	Con questa versione, AWS Config supporta la seguente regola gestita: efs-mount-target-public-accessible	20 marzo 2024
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • dms-neptune-iam-authorization-enabled • autenticazione dms-mongo-db abilitata • abilitato a dms-redis-tls • crittografia dax-tls-endpoint • eks-cluster-secrets-criptato • kinesis-firehose-delivery-stream crittografato • abilitato per mq-cloudwatch-audit-log • abilitato per mq-cloudwatch-audit-log • opensearch-primary-node-fault-tolerance • sagemaker-endpoint-config-prod-instance-count • catalogo di servizi condiviso all'interno dell'organizzazione • transfer-family-server-no-ftp	26 febbraio 2024

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Managed Service for Prometheus, Amazon, Amazon CloudWatch Cognito, Amazon, Amazon FSx, AWS Identity and Access Management (IAM) ElastiCache,, Amazon AWS RAM Redshift Serverless AWS Lambda, Amazon e Amazon AWS Glue Simple Notification Service (Amazon SNS). SageMaker Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	22 febbraio 2024
AWS Config aggiorna le regole gestite	Con questa versione, AWS Config supporta la seguente regola gestita: s3-bucket-cross-region-replication-enabled	12 febbraio 2024

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione su nuovi AWS AppConfig , Amazon CloudWatch Evidently, AWS Identity and Access Management (IAM), Amazon MemoryDB for Redis (MemoryDB), Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Redshift e tipi di risorse. AWS Transfer Family Per ulteriori informazi oni, consulta Tipi di risorsa supportati.	6 febbraio 2024
AWS Config aggiorna le regole gestite	Con questa versione, AWS Config supporta la seguente regola gestita: macie-auto-sensitive-data-discovery-check	29 gennaio 2024

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione dei nuovi Amazon AppStream, AWS Key Management Service (AWS KMS), Amazon Relational Database Service (Amazon RDS), Amazon Cognito, Amazon Elastic Compute Cloud (Amazon EC2), EC2 Image Builder AWS Ground Station,, Amazon, Amazon Redshift e tipi di risorse. AWS Mainframe Modernization QuickSight AWS Systems Manager Per ulteriori informazioni, consulta Tipi di risorsa supportati.	3 gennaio 2024

I limiti di servizio aumentano per il numero massimo di regole per regione per account AWS Config	Con questa versione, AWS Config supporta 1000 AWS Config regole per AWS regione per account. Questo aumento si applica al totale di tutte le regole implement ate, tra cui regole AWS Config gestite, regole AWS Config personalizzate, pacchetti di AWS Config conformità, AWS Security Hub controlli, AWS Firewall Manager politiche e piani di AWS Backup backup per regione e account. Per ulteriori informazioni, consulta la pagina relativa alle restrizio ni dei servizi .	19 dicembre 2023

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • s3-meets-restore-time-target • ebs-meets-restore-time-target • ec2-meets-restore-time-target • rds-meets-restore-time-target • efs-meets-restore-time-target • fsx-meets-restore-time-target • aurora-meets-restore-time-target • dynamodb-meets-restore-time-target	19 dicembre 2023

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Managed Service for Prometheus AWS AppConfig, () AWS Database Migration Service , AWS DMS(AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Logs CloudWatch e Amazon Simple Storage Service (Amazon S3). AWS Organizations Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	5 dicembre 2023

Versione di anteprima : processore di query in linguaggio naturale per query avanzate	Con questa versione, è possibile utilizzare il processor e di query in linguaggio naturale per query avanzate, che utilizza funzionalità di intelligenza artificiale generativa (AI generativa) che consentono di porre domande in un inglese semplice e convertirle in un formato di ready-to-use query. Con il processore di interrogazioni in linguaggio naturale, puoi interrogare la tua Account AWS o l'intera organizzazione. AWS Per ulteriori informazi oni, consulta Natural language interrogation processor for advanced query.	26 novembre 2023

Registrazione periodica	Con questa versione, AWS Config supporta la registrazione periodica. La registrazione periodica offre la possibilità di acquisire le ultime modifiche alla configurazione delle risorse in un determinato periodo di tempo. Ora è possibile impostare la frequenza predefinita per la registrazione della configyrazione su Giornaliera, consentendo così di ricevere un elemento di configurazione (CI) che rappresenta lo stato più recente delle risorse nelle ultime 24 ore, solo se è diverso dall'elemento della configurazione registrato in precedenza. La AWS Config console introduce anche una nuova esperienza di strategia di registrazione, in cui è anche possibile sovrascrivere la frequenza di registrazione per tipi di risorse specifici o escludere tipi di risorse specifici dalla registrazione. In questo modo è possibile adattare le impostazioni ai requisiti granulari. Sono stati aggiunti i seguenti tipi di dati: • RecordingMode • RecordingModeSostituisci	26 novembre 2023

Sono stati aggiornati i seguenti tipi di dati:

- PutConfigurationRegistratore
- ConfigurationRecorder
- BaseConfigurationArticolo
- ConfigurationItem

Sono state aggiornate le seguenti pagine della guida per gli sviluppatori:

- Risorse di ricodifica AWS
- Configurazione AWS Config con la AWS Config console | Configurazione con 1 clic
- Configurazione AWS Config con la AWS Config console | Configurazione manuale
- Configurazione AWS Config con la AWS CLI

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Cognito, Amazon Connect, Amazon EMR, AWS Ground Station AWS Mainframe Modernization, Amazon MemoryDB for Redis, Amazon AWS Organizations, Amazon QuickSight Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53 e. AWS Service Catalog AWS Transfer Family Le policy `AWSConfigServiceRolePolicy` e `AWS_ConfigRole` ora aggiungono anche identificatori di sicurezza (SID) per le policy `AWSConfigServiceRolePolicyStatementID`, `AWSConfigSLRLogStatementID`, `AWSConfigSLRLogEventStatementID`, `AWSConfigSLRApiGatewayStatementID` e `AWSConfigServiceRolePolicy`.	17 novembre 2023

	Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • acm-pca-root-ca-disabled • dynamodb-table-deletion-protection-enabled • ec2-client-vpn-connection-log-enabled • eks-cluster-log-enabled • emr-block-public-access • fsx-windows-audit-log-configured • fsx-openzfs-copy-tags-enabled • fsx-lustre-copy-tags-to-backups • msk-enhanced-monitoring-enabled • mq-auto-minor-version-upgrade-enabled • neptune-cluster-multi-az-enabled • opensearch-update-check • s3-access-point-in-vpc-only • s3-access-point-public-access-blocks • s3-bucket-mfa-delete-enabled	9 novembre 2023

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione di nuovi AWS Identity and Access Management (IAM), () AWS Network Manager, AWS Private Certificate Authority Amazon Connect AWS App Mesh, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS), Amazon AWS IoT Managed Streaming AWS IoT TwinMaker for Apache Kafka Connect (Amazon MSK Connect) Connect) e tipi di risorse.AWS Private CA AWS Lambda Esploratore di risorse AWS Per ulteriori informazi oni, consulta Tipi di risorsa supportati.	3 novembre 2023
AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config aggiorna il seguente pacchetto di conformità: Operational Best Practices for BNM RMit	26 ottobre 2023

Pannelli di controllo della conformità e dell'inventario per gli aggregatori	Con questa versione, AWS Config aggiunge una pagina dashboard di conformità e una pagina dashboard di inventario alla visualizzazione aggregata della console. AWS Config Nella pagina del pannello di controllo della conformità, puoi visualizzare pannelli di controllo automatici con widget di riepilogo delle informazi oni sulla conformità delle risorse all'interno dell'aggr egatore, ad esempio i primi 10 tipi di risorse per risorse non conformi, i primi 10 pacchetti di conformità a livello di account per regole non conformi e altro ancora. Nella pagina del pannello di controllo dell'inventario, puoi visualizzare pannelli di controllo automatici con widget di riepilogo delle informazioni sui dati di configurazione delle risorse all'interno dell'aggr egatore, ad esempio i primi 10 tipi di risorse in base al numero di risorse, i primi 10 account in base al numero di risorse e altro ancora. Per informazioni sul grafo e i grafici, consulta Pannello di controllo della conformità e	23 ottobre 2023

	Pannello di controllo dell'inventario.	
Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Connect AWS Private CA AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Evidently, Amazon Managed Grafana, Amazon, Amazon Inspector e Amazon GuardDuty AWS IoT Managed AWS IoT TwinMaker Streaming for Apache Kafka (Amazon MSK) e Amazon. AWS Lambda AWS Network Manager AWS Organizations SageMaker Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	4 ottobre 2023

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione di nuovi tipi di AWS IoT risorse AWS IoT TwinMaker Amazon Personalize Amazon Managed Streaming for Apache Kafka (Amazon MSK) SageMaker, Amazon, Amazon e AWS CodeBuild Amazon AppStream Inspector. AWS IoT Wireless Per ulteriori informazioni, consulta Tipi di risorsa supportati.	4 ottobre 2023

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • docdb-cluster-deletion-protection-enabled • docdb-cluster-audit-logging-enabled • docdb-cluster-snapshot-public-prohibited • mq-active-deployment-mode • mq-rabbit-deployment-mode • dms-auto-minor-version-upgrade-check • dms-replication-task-target db-logging • dms-replication-task-source db-logging • dms-endpoint-ssl-configured • custom-eventbus-policy-attached • global-endpoint-event-replication-enabled • route53-query-logging-enabled • rds-aurora-mysql-audit-logging-enabled • rds-cluster-auto-minor-version-upgrade-enable • appsync-authorization-check • netfw-deletion-protection-enabled	21 settembre 2023

	• wafv2-rulegroup-logging-enabled • msk-in-cluster-node-require-tls	
AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config aggiorna i seguenti pacchetti di conformità: • Best practice operative per Amazon S3 • Best practice operative per EC2	8 settembre 2023
Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy ora rimuove le autorizzazioni per AWS Systems Manager (Systems Manager). Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	6 settembre 2023
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione di nuovi Amazon CodeGuru Profiler, AWS Elemental MediaConnect AWS Transfer Family, Amazon Managed Service for Prometheus AWS Batch e tipi di risorse. AWS Cloud Map Amazon Route 53 Resolver Per ulteriori informazioni, consulta Tipi di risorsa supportati.	6 settembre 2023

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • athena-workgroup-encrypted-at-rest • neptune-cluster-iam-database-authentication • neptune-cluster-copy-tags-to-snapshot-enabled • neptune-cluster-cloudwatch-log-export-enabled • neptune-cluster-deletion-protection-enabled • neptune-cluster-snapshot-encrypted • neptune-cluster-backup-retention-check • neptune-cluster-encrypted • neptune-cluster-snapshot-public-prohibited • docdb-cluster-backup-retention-check • docdb-cluster-encrypted • rds-cluster-encrypted-at-rest	10 agosto 2023

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione di nuovi Amazon AWS Amplify, Amazon Athena AppIntegrations AWS App Mesh, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Evidently CloudWatch , Amazon Forecast,,,, Amazon Managed AWS Elemental MediaConvert Streaming AWS Elemental MediaTailor for Apache Kafka (Amazon MSK) AWS IoT Greengrass Version 2 AWS Ground Station, Amazon Personalize, Amazon Pinpoint Amazon Pinpoint e tipi di risorse. AWS Resilience Hub Per ulteriori informazioni, consulta Tipi di risorsa supportati.	3 agosto 2023

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Managed Workflows for, AWS App Mesh Amazon AppStream 2.0, AWS CloudFormation Amazon Connect CloudFront AWS CodeArtifact, Amazon AWS CodeBuild, AWS Identity and Access Management (IAM), AWS Glue Amazon Inspector GuardDuty,,, Amazon Managed Streaming for Apache Kafka AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon Macie,,,,, Amazon Route 53, Amazon Simple Storage Service (Amazon AWS Elemental MediaConnect S3) Storage Service S3 AWS Network Manager AWS Organizations Esploratore di risorse AWS, Amazon Simple Notification Service (Amazon SNS) e sistemi Amazon EC2 Manager (SSM). Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	28 luglio 2023

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzarla AWS Config per registrare le modifiche alla configurazione dei nuovi Amazon Kinesis, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Simple Storage Service (Amazon S3), Amazon Virtual Private Cloud (Amazon VPC), Amazon Kendra, Amazon Connect Tipi di risorse Amazon Connect,, , e (). AWS CloudFormation AWS AppConfig AWS App Mesh AWS App Runner AWS Database Migration Service AWS DMS Per ulteriori informazioni, consulta Tipi di risorsa supportati.	10 luglio 2023
Aumento delle restrizioni dei servizi per i pacchetti di conformità dell'organizzazione	Con questa versione, AWS Config supporta 350 AWS Config regole per regione per account in tutti i pacchetti di conformità e 350 regole organizzative per organizza zione. AWS Config Per ulteriori informazioni, consulta la pagina relativa alle restrizio ni dei servizi .	13 giugno 2023

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Managed Workflows for AWS Amplify, Amazon Connect, AWS App Mesh Amazon Managed Service for Prometheus, Amazon Athena,,,, Amazon, Amazon AWS Directory Service DynamoDB AWS Batch AWS CloudFormation AWS CodeArtifact, AWS CloudTrail Amazon Elastic Compute Cloud (CodeGuruAmazon EC2), Amazon Evidently, Amazon Forecast,,, (AWS Ground Station IAM), Amazon Managed Streaming per Apache Kafka AWS IoT Greengrass(CloudWatch Amazon MSK AWS Identity and Access Management) AWS Organizations, Amazon Lightsail, Amazon Logs, CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC), Amazon Personalize, Amazon QuickSight, Amazon Simple Storage Service (AWS Migration Hub Refactor	13 giugno 2023

Spaces Amazon S3), Amazon e. SageMaker AWS Transfer Family Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.

AWS Config Esclusioni di registrazione per tipo di risorsa	Con questa versione, AWS Config consente di escludere tipi specifici di AWS risorse dal monitoraggio dell'inventario e dalla conformità, pur continuando a tenere traccia di tutti gli altri tipi di risorse supportati attualmente disponibili AWS Config, compresi quelli che verranno aggiunti in futuro. Puoi utilizzare questa funzionalità per concentrarti sulle risorse critiche soggette agli standard di conformità e governance in vigore. Gli aggiornamenti all'API per il registratore di configurazione e il gruppo di registrazione sono retrocompatibili, il che significa che funzionano con le versioni precedenti dell'API PutConfigurationRecorder. Puoi continuare a gestire i tipi di risorse da registrare esattamente nello stesso modo di prima, senza utilizzare le API nuove o aggiornate. Sono stati aggiunti i seguenti tipi di dati: • RecordingStrategy • ExclusionByResourceTypes Sono stati aggiornati i seguenti tipi di dati:	9 giugno 2023

	• PutConfigurationRegistratore • ConfigurationRecorder • RecordingGroup È stata aggiornata la seguente pagina della guida per gli sviluppatori: • Scegli quali risorse devono essere registrate	
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione del nuovo Amazon Elastic Container Service (Amazon ECS), Amazon Keyspaces (per Apache Cassandra) (Amazon Keyspaces),,,, Amazon 2.0 AWS Signer AWS Amplify AWS App Mesh, AWS App Runner Amazon Elastic Compute Cloud (AppStream Amazon EC2) AWS CodeArtifact, Amazon CloudWatch Evidently, Amazon Forecast, (AWS Identity and Access Management IAM), Amazon Pinpoint, Amazon, tipi di risorse Amazon Data Firehose. SageMaker AWS Transfer Family Per ulteriori informazioni, consulta Tipi di risorsa supportati.	5 giugno 2023

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • cloudfront-s3-origin-access-control-enabled • custom-schema-registry-policy-attached • ec2-client-vpn-not-authorize-all • elasticache-supported-engine-version • macie-status-check • mq-automatic-minor-version-upgrade-enabled • mq-cloudwatch-audit-logging-enabled • netfw-logging-enabled • opensearch-encrypted-at-res • step-functions-state-machine-logging-enabled	10 maggio 2023

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione di nuovi Amazon Route 53 Resolver Amazon Elastic Compute Cloud (Amazon EC2) AWS IoT , Wireless,,,, Amazon, Amazon Redshift AWS Network Manager AWS Device Farm, AWS Ground Station Amazon Pinpoint, , AppFlow AWS AppConfig EC2 Image Builder, Amazon AWS IoT, Amazon Runtime, CloudWatch Amazon AWS Panorama ECR e tipi di risorse. SageMaker AWS Audit Manager Per ulteriori informazioni, consulta Tipi di risorsa supportati.	5 maggio 2023
AWS Config supporta nuovi tipi di risorse	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione di`AWS::NetworkFirewall::TLSInspectionConfiguration` . Per ulteriori informazioni, consulta Tipi di risorsa supportati.	1 maggio 2023

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Managed Workflows for AWS Amplify AWS App Mesh,, AWS App Runner AWS CodeArtifact Amazon CloudFront,, Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon, Amazon AWS Migration Hub Pinpoint, AWS Resilience AWS Transfer Family Hub, Amazon, Directory Service e. SageMaker CloudWatch AWS AWS WAF Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	13 aprile 2023

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • elasticache-auto-minor-version-upgrade-check • elasticache-repl-grp-auto-failover-enabled • elasticache-repl-grp-encrypted-at-rest • elasticache-repl-grp-encrypted-in-transit • elasticache-repl-grp-redis-auth-enabled • elasticache-subnet-group-check • cloudfront-s3-origin-non-existent-bucket	10 aprile 2023
Aumento delle restrizioni dei servizi per i pacchetti di conformità dell'organizzazione	Con questa versione, AWS Config supporta 350 AWS Config regole per account in tutti i pacchetti di conformità dell'organizzazione. Per ulteriori informazioni, consulta la pagina relativa alle restrizioni dei servizi .	3 aprile 2023

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • acm-certificate-rsa-check • appsync-associated-with-waf • appsync-logging-enabled • elasticache-rbac-auth-enabled • mq-no-public-access • netfw-multi-az-enabled • ses-malware-scanning-enabled • eks-cluster-logging-enabled • appsync-cache-encryption-at-rest	3 aprile 2023

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione del nuovo streaming video Amazon AppStream 2.0, AWS Auto Scaling, Amazon Connect Amazon Elastic Compute Cloud, Amazon, HealthLake Kinesis EventBridge, Lookout AWS IoT TwinMaker for Vision, Network Manager, Amazon Pinpoint, Amazon Route 53 Application Recovery Controller e tipi di risorse. AWS RoboMaker Per ulteriori informazioni, consulta Tipi di risorsa supportati.	3 aprile 2023

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Managed Workflows for Amazon AppFlow, AWS App Runner Amazon AppStream 2.0, AWS CloudFormation Amazon,,, CloudWatch AWS CodeArtifact, CloudFront Amazon Elastic Compute Cloud (AWS Device Farm Amazon EC2) AWS CodeCommit, Amazon Evidently, Amazon Forecast, AWS Identity and Access Management (IAM) CloudWatch , Amazon MemoryDB for Redis AWS Ground Station, Amazon Pinpoint, AWS IoT Amazon Relational Database AWS Network Manager Service Database Relational (Amazon RDS), Amazon Redshift e AWS Panorama Amazon. SageMaker Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	30 marzo 2023

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` politica e la `AWS_ConfigRole` politica ora concedono autorizzazioni aggiuntive per AWS Audit Manager. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	3 marzo 2023
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione su nuovi Amazon AWS Elemental MediaPackage EventBridge AWS IoT, (Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Lookout for Metrics, Amazon CodeGuru Lex, AWS Device Farm, Amazon Budget AWS Reviewer e tipi di risorse. Amazon Route 53 Resolver AWS RoboMaker Per ulteriori informazioni, consulta Tipi di risorsa supportati.	2 marzo 2023
Aggiornamento IAM di sicurezza	AWS Config ora tiene traccia delle modifiche alla policy. `AWSConfigMultiAccountSetupPolicy` Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	27 febbraio 2023

AWS Config Copertura delle risorse per regione e disponibilità	Con questa versione, AWS Config fornisce informazioni sulla regione per ogni tipo di risorsa supportata. Per informazioni sui tipi di risorse supportati nelle varie regioni, consulta Copertura delle risorse in base alla disponibilità nelle regioni.	20 febbraio 2023
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione dei nuovi Amazon Interactive Video Service (Amazon IVS), Amazon Simple Storage Service (Amazon S3), Amazon Elastic Kubernetes Service AWS Glue(Amazon EKS) e Amazon Relational Database Service (Amazon RDS) AWS IoT e Managed Service for Apps Tipi di risorse Ache Flink. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	7 febbraio 2023

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Managed Workflows for Apache Airflow, AWS IoT Amazon 2.0 AppStream , Amazon CodeGuru Reviewer, Amazon Kinesis AWS HealthLake Video Streams, Amazon Route 53 Application Recovery Controller, Amazon Elastic Compute Cloud (Amazon EC2) AWS Device Farm, Amazon Pinpoint (IAM), Amazon e Amazon Logs. AWS Identity and Access Management GuardDuty CloudWatch Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	1 febbraio 2023
Aggiornamento IAM di sicurezza	Come best practice di sicurezza, la policy `ConfigConformsServiceRolePolicy` ora rimuove l'autorizzazione ampia a livello di risorsa per `config:DescribeConfigRules` . Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	12 gennaio 2023

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Managed Service for Prometheus AWS Audit Manager,,, (), AWS Device Farm Amazon Elastic Compute Cloud AWS Database Migration Service (Amazon EC2 AWS DMS) AWS Directory Service, Amazon Lightsail,, Amazon, Amazon, Amazon, Amazon Application Recovery Controller AWS Glue AWS IoT, Amazon Route 53 Application Recovery Controller AWS Elemental MediaPackage AWS Network Manager, Amazon Simple Storage Service (QuickSight AWS Resource Access Manager Amazon S3), e Amazon Timestream. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	10 gennaio 2023

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione di nuovi EventBridge schemi Amazon MQ, AWS AppConfig, AWS Cloud9, Amazon Fraud Detector,, Amazon Lightsail AWS IoT AWS IoT Analytics , MediaPackage (), Amazon Route 53 Application Recovery AWS Resilience Hub Controller e tipi di risorse. AWS Elemental MediaPackage AWS Transfer Family Per ulteriori informazioni, consulta Tipi di risorsa supportati.	5 gennaio 2023
AWS Config regola la copertura delle risorse	In questa versione, AWS Config visualizza la copertura dei tipi di risorse per un numero maggiore di regole AWS Config gestite.	21 dicembre 2022
AWS Config individuabilità delle regole	In questa versione, AWS Config supporta le pagine per Elenco delle regole AWS Config gestite per modalità di valutazione, Elenco delle regole AWS Config gestite per tipo di trigger e Elenco delle regole AWS Config gestite per disponibilità regionale.	21 dicembre 2022

AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config aggiorna i seguenti pacchetti di conformità: • Best practice operative per K-ISMS • Best practice operative per NIST 800 171 • Best practice operative per PCI DSS 3.2.1 • Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello alto • Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello medio • Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello basso • Best practice operative per NZISM • Best practice operative per NIST 800-53 rev 5	19 dicembre 2022

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • api-gwv2-access-logs-enabled • api-gwv2-authorization-type-configured • cloudfront-security-policy-check • ec2-launch-template-public-ip-disabled • elastic-beanstalk-logs-to-cloudwatch • sagemaker-notebook-instance-inside-vpc • sagemaker-notebook-instance-root-access-check • security-account-information-provided • storagegateway-resources-protected-by-backup-plan • wafv2-rulegroup-not-empty • wafv2-webacl-not-empty	9 dicembre 2022

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione dei nuovi tipi di risorse Amazon CloudWatch RUM EventBridge, Amazon GuardDuty, Amazon, Amazon AWS Backup Simple Email Service (Amazon SES) AWS Fault Injection Service e AWS FIS(). AWS DataSync Per ulteriori informazioni, consulta Tipi di risorsa supportati.	9 dicembre 2022

AWS Config Conformità proattiva	Con questa versione, AWS Config supporta la capacità di verificare in modo proattivo la conformità alle AWS Config regole prima dell'appr ovvigionamento delle risorse. Ciò consente di valutare le impostazioni di configura zione delle risorse esistenti prima che vengano create o aggiornate. AWS Config Utilizzatelo per tenere traccia delle modifiche alla configura zione apportate alle risorse, prima o dopo il provision ing, e verificare se le risorse corrispondono alle configura zioni desiderate. Sono stati aggiunti i seguenti tipi di dati: • GetResourceEvaluat ionSummary • StartResourceValutazione • ListResourceValutazioni Sono stati aggiornati i seguenti tipi di dati: • DescribeConfigRulesFilters • GetComplianceDetai lsByRisorsa • EvaluationResultQualificato re	28 novembre 2022

- EvaluationModeConfigurazione

Sono state aggiornate le seguenti pagine della guida per gli sviluppatori:

- Componenti di una AWS Config regola
- Modalità di valutazione e tipi di trigger per AWS Config le regole
- AWS Config Regole gestite
- AWS Config Regole personalizzate
- Gestione delle AWS Config regole

Drift Detection come elemento di configurazione (CI) per il AWS Config Configuration Recorder	In questa versione, AWS Config tiene traccia di tutte le modifiche al registratore di configurazione per indicare se lo stato del registratore di configurazione è diverso o si è spostato rispetto allo stato precedente; ad esempio, se vi sono aggiornamenti ai tipi di risorse di cui avete abilitato AWS Config la registrazione, se avete arrestato o avviato il registratore di configurazione o se avete eliminato o disinstallato il registratore di configurazione. Il tipo di `AWS::Config::ConfigurationRecorder` risorsa è un tipo di risorsa di sistema AWS Config e la registrazione di questo tipo di risorsa è abilitata per impostazione predefinita in tutte le regioni supportate. La registrazione del tipo di risorsa `AWS::Config::ConfigurationRecorder` è disponibile senza costi aggiuntivi. Per ulteriori informazioni, consulta Rilevamento deviazione del registratore di configurazione.	18 novembre 2022

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione di nuovi AWS IoT Events tipi di risorse EC2 Image AWS DataSync Builder AWS Glue,, Amazon Route 53 Application Recovery Controller e Amazon Elastic Container Registry (Amazon ECR). AWS Cloud Map Per ulteriori informazioni, consulta Tipi di risorsa supportati.	8 novembre 2022
Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per. AWS CloudFormation Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	7 novembre 2022

AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta i seguenti pacchetti di conformità: • Best practice operative per Criminal Justice Information Services (CJIS) • Best practice di sicurezza per Amazon SageMaker • Best practice di sicurezza per Amazon Elastic Container Registry Sono stati aggiornati i seguenti pacchetti di conformità: • Best practice operative per MAS TRMG • Best practice operative per NCSC Cyber Assessment Framework • Best practice operative per i principi di sicurezza cloud NCSC	27 ottobre 2022

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per AWS Certificate Manager Amazon Managed Workflows for Apache Airflow, AWS Amplify Amazon Keyspaces, Amazon, AWS AppConfig Amazon Connect, Amazon Elastic Compute Cloud (CloudWatchAmazon EC2) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon Amazon FSx EventBridge, AWS Fault Injection Service Amazon, Amazon Location Service, Amazon Lex, Amazon Lightsail, GameLift Amazon Pinpoint, Amazon AWS IoT, Amazon Relational AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Servizio di database (Amazon RDS), Amazon AWS RoboMaker Rekognition,, Amazon Route 53 AWS Resource Groups, Amazon Simple Storage Service (Amazon S3) e. AWS Cloud Map AWS Security	19 ottobre 2022

	Token Service Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione dei nuovi Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Email Service (Amazon SES) Simple Email Service (Amazon AWS AppConfig SES) e tipi di risorse. AWS Cloud Map AWS DataSync Per ulteriori informazioni, consulta Tipi di risorsa supportati.	6 ottobre 2022
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzarla AWS Config per registrare le modifiche alla configurazione di nuovi Amazon GuardDuty SageMaker AWS AppSync AWS Cloud Map, Amazon e tipi di AWS DataSync risorse. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	4 ottobre 2022
AWS Config supporta un nuovo pacchetto di conformità	Con questa versione, AWS Config aggiorna il pacchetto di conformità Operational Best Practices for SWIFT CSP.	4 ottobre 2022

AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta i seguenti pacchetti di conformità: • Best practice operative per CMMC 2.0 – Livello 1 • Best practice operative per CMMC 2.0 – Livello 2 Sono stati aggiornati i seguenti pacchetti di conformità: • Best practice operative per Gateway Amazon API • Best practice operative per AWS Well-Architected Framework Reliability Pillar • Best practice operative per AWS Well-Architected Framework Security Pillar • Best practice operative per CMMC – Livello 1 • Best practice operative per CMMC – Livello 2 • Best practice operative per CMMC – Livello 3 • Best practice operative per CMMC – Livello 4 • Best practice operative per CMMC – Livello 5 • Best practice operative per FFIEC • Best practice operative per FedRAMP(Low)	30 settembre 2022

	• Best practice operative per MAS Notice 655 • Best practice operative per NBC TRMG • Best practice operative per NIST 800 172	
Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per. AWS Glue Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	14 settembre 2022
AWS Config supporta il nuovo pacchetto di conformità	Con questa versione, AWS Config supporta il pacchetto di conformità Operational Best Practices for SWIFT CSP.	9 settembre 2022

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon Guru, DevOps Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon Amazon FinSpace Schems Amazon Fraud Detector, Amazon, EventBridge Amazon Interactive Video Service (EventBridge Amazon IVS), Servizio gestito da Amazon per Apache Flink GameLift, EC2 Image Builder, Amazon Lex, Amazon Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble QuickSight Pinpoint, Amazon, StudioAmazon Amazon, Controller di ripristino delle applicazioni Amazon Route 53, Amazon Simple Storage	7 settembre 2022

Service (Amazon S3) S3) Amazon Route 53 Resolver, Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestrea m,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup Budget AWS AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events, AWS IoT SiteWise, AWS IoT TwinMaker, AWS Lake Formation AWS License Manager, AWS Resilience Hub, AWS Signer, e AWS Transfer Family. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.

AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta i seguenti pacchetti di conformità: • Best practice operative per Amazon CloudWatch • Best practice operative per il Cloud Computing Compliance Controls Catalog (C5) in Germania • Best practice operative per IRS 1075 Sono stati aggiornati i seguenti pacchetti di conformità: • AWS Pacchetto di conformità Control Tower Detective Guardrails • Best practice operative per CISA Cyber Essentials • Best practice operative per la guida alla cibersicurezza dell'ENISA per le PMI • Best practice operative per FDA Titolo 21 CFR Parte 11 • Best practice operative per FedRAMP (Moderato) • Best practice operative per la sicurezza HIPAA • Best practice operative per NIST Privacy Framework v1.0 • Best practice operative per NYDFS 23	31 agosto 2022

	• Best practice operative per RBI Cyber Security Framework per UCB • Best practice operative per RBI MD-ITF	
Guida introduttiva AWS Config e aggiornamenti del Custom Conformance Pack	Con questa versione, AWS Config aggiorna le pagine Guida introduttiva AWS Config e Configurazione AWS Config con la console, introducendo una pagina di configurazione con un clic e una pagina di configurazione manuale. AWS Config aggiorna inoltre la pagina Custom Conformance Pack con una procedura dettagliata su come creare un file YAML del Conformance Pack partendo da zero.	25 agosto 2022

AWS Systems Manager Integrazione del documento (documento SSM) con i Conformance Pack	Con questo rilascio, puoi creare un modello di pacchetto di conformità con un documento SSM. Per ulteriori informazioni sui documenti SSM, consulta Documenti AWS Systems Manager nella Guida per l'utente di AWS Systems Manager . Sono stati aggiornati i seguenti tipi di dati: • PutConformancePacchetto • ConformancePackDettaglio • ModelliSSM DocumentDetails Sono state aggiornate le seguenti pagine della guida per gli sviluppatori: • Distribuzione di un Conformance Pack tramite la console AWS Config • Distribuzione di un Conformance Pack utilizzando l'interfaccia a riga di comando AWS	24 agosto 2022

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Simple Email Service (Amazon SES) AWS DataSync, e. AWS Cloud Map Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	22 agosto 2022
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione dei nuovi tipi di risorse Amazon Athena, Amazon Detective, SageMaker Amazon, Amazon Route 53, AWS Database Migration Service (AWS DMS) AWS Glue, AWS Key Management Service (AWS KMS) e Amazon Simple Email Service (Amazon SES). Per ulteriori informazioni, consulta Tipi di risorsa supportati.	16 agosto 2022

AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config aggiorna i seguenti pacchetti di conformità: • Best practice operative per NIST 1800 25 • Best practice operative per NIST 800 181 • Best practice operative per ABS CCIG 2.0 Standard Workloads • Best practice operative per ABS CCIG 2.0 Material Workloads • Best practice operative per ACSC Essentials 8 • Best practice operative per ACSC ISM • Best practice operative per APRA CPG 234 • Migliori pratiche operative per CIS AWS Foundations Benchmark v1.4 Level 1 • Migliori pratiche operative per CIS AWS Foundations Benchmark v1.4 Level 2 • Best practice operative per BNM RMiT • Best practice operative per NIST CSF	1 agosto 2022

Punteggio di conformità per i pacchetti di conformità	Con questa versione, AWS Config introduce il punteggio di conformità per i pacchetti di conformità, che offre una visione di alto livello dello stato di conformità dei pacchetti di conformità. È possibile utilizzar lo per identificare, analizzar e e comprendere il livello di conformità dei pacchetti di conformità. Il punteggio di conformità è la percentua le del numero di combinazi oni regola-risorsa conformi in un pacchetto di conformit à rispetto al numero totale di combinazioni regola-risorsa possibili nel pacchetto di conformità. Sono stati aggiornati i seguenti tipi di dati: • ListConformancePac kCompliancePunteggi • ConformancePackCom plianceScore Sono state aggiornate le seguenti pagine della guida per gli sviluppatori: • Visualizzazione del AWS Config pannello di controllo • Visualizzazione dei dati di conformità nel pannello di	26 luglio 2022

	controllo dei pacchetti di conformità • Gestione dei pacchetti di conformità (API)	
Aggiornamento IAM di sicurezza	La `ConfigConformsServiceRolePolicy` policy ora concede l'autorizzazione a pubblicare punti dati metrici su Amazon. CloudWatch Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	25 luglio 2022

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Elastic Container Service (Amazon ECS), Amazon, Amazon, Amazon FSx, ElastiCache EventBridge Amazon Managed Service per Apache Flink, Amazon Location Service, Amazon Managed Streaming per Apache Kafka, Amazon, Amazon, Amazon Rekognition, Amazon Rekognition, Amazon Simple Storage Service (Amazon S3) AWS RoboMaker, Amazon Simple Email Service (Amazon SES),,,,,,, (IAM Identity Center), EC2 Image Builder, QuickSight AWS Amplify AWS AppConfig AWS AppSync AWS Billing Conductor AWS DataSync AWS Firewall Manager AWS Glue AWS IAM Identity Center e Elastic Load Balancing. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	15 luglio 2022

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione dei nuovi tipi di risorse Amazon Elastic Compute Cloud (Amazon EC2). Per ulteriori informazi oni, consulta Tipi di risorsa supportati.	8 luglio 2022
AWS Config supporta nuovi tipi di risorse	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione di nuovi tipi di AWS Global Accelerator risorse. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	5 luglio 2022
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • autoscaling-launch-template • ecs-task-definition-log-configuration • ecs-awsvpc-networking-enabled • nlb-cross-zone-load-balancing-enabled	1 luglio 2022

AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta i seguenti pacchetti di conformità: • Best practice operative per il Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile • Best practice operative per il Gramm Leach Bliley Act (GLBA) • Best practice operative per GxP dell'Allegato 11 dell'UE • Best practice di sicurezza per Amazon Elastic Kubernetes Service (Amazon EKS) • Best practice di sicurezza per Amazon Relational Database Service (Amazon RDS) • Best practice di sicurezza per AWS Lambda Sono stati aggiornati i seguenti pacchetti di conformità: • Best practice operative per IA e ML • Best practice operative per Amazon DynamoDB • Best practice operative per CIS Critical Security Controls v8 IG1	30 giugno 2022

	• Best practice operative per CIS Critical Security Controls v8 IG2 • Best practice operative per CIS Critical Security Controls v8 IG3 • Best practice operative per la sicurezza HIPAA • Best practice operative per NIST 800-53 rev 5 • Best practice operative per NIST CSF	
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzarla AWS Config per registrare le modifiche alla configurazione di nuovi tipi di SageMaker risorse Amazon. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	29 giugno 2022

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione dei nuovi tipi di risorse Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Route 53, WorkSpace s AWS Batch Amazon, (IAM Access Analyzer AWS Database Migration Service) AWS Identity and Access Management Access Analyzer AWS DMS, () AWS Step Functions ed Elastic Load Balancing. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	14 giugno 2022

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • aurora-last-backup-recovery-point-created • dynamodb-last-backup-recovery-point-created • ebs-last-backup-recovery-point-created • ec2-last-backup-recovery-point-created • efs-last-backup-recovery-point-created • fsx-last-backup-recovery-point-created • rds-last-backup-recovery-point-created • s3-last-backup-recovery-point-created • storagegateway-last-backup-recovery-point-created • virtualmachine-last-backup-recovery-point-created	13 giugno 2022

AWS Config Integrazione con AWS Security Hub	Con questa versione, è possibile visualizzare i risultati delle valutazioni AWS Config gestite e personalizzate delle regole come risultati in AWS Security Hub. Security Hub trasforma le valutazioni delle regole in esiti in grado di fornire ulteriori informazioni, come il nome della risorsa Amazon (ARN) e la data di creazione, sulle risorse interessate. Questi esiti possono essere visualizz ati insieme ad altri esiti di Security Hub, per fornire una panoramica completa della posizione di sicurezza. Per ulteriori informazioni, consulta Invio delle valutazioni delle regole a Security Hub	7 luglio 2022

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per Amazon Athena, Amazon Detective, GuardDuty Amazon, Amazon Macie, Amazon Simple Email Service (Amazon SES), () AWS Glue e. AWS Resource Access Manager AWS RAM AWS IAM Identity Center Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	31 maggio 2022
AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta i seguenti pacchetti di conformità: • Best practice di sicurezza per Amazon Elastic Container Service (Amazon ECS) • Best practice di sicurezza per Amazon Elastic File System (Amazon EFS) • Best practice di sicurezza per Amazon CloudFront • Best practice di sicurezza per AWS Auto Scaling • Best practice di sicurezza per AWS Network Firewall • Best practice di sicurezza per AWS Secrets Manager	31 maggio 2022

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzarla AWS Config per registrare le modifiche alla configurazione di nuovi tipi di AWS Step Functions risorse SageMaker e Amazon. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	26 maggio 2022
AWS Config supporta un nuovo pacchetto di conformità	Con questa versione, AWS Config aggiorna il pacchetto di conformità Operational Best Practices for NERC CIP BCSI.	20 maggio 2022
AWS Config Componenti di una regola	Con questa versione, AWS Config introduce una pagina Componenti di una AWS Config regola. La pagina illustra la struttura delle definizioni delle regole, i metadati delle regole e le migliori pratiche su come scrivere regole con Python utilizzando il Rules Developme nt Kit (RDK) e la AWS Config Rules Development Kit Library (AWS Config RDKLib).	9 maggio 2022
Aumento delle restrizioni dei servizi per i pacchetti di conformità dell'organizzazione	Con questa versione, AWS Config supporta 180 AWS Config regole per account in tutti i pacchetti di conformit à dell'organizzazione. Per ulteriori informazioni, consulta la pagina relativa alle restrizio ni dei servizi .	6 maggio 2022

AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta i seguenti pacchetti di conformità: • Best practice di sicurezza per Amazon OpenSearch Service • Best practice di sicurezza per Amazon Redshift • Best practice di sicurezza per AWS CloudTrail • Best practice di sicurezza per AWS CodeBuild • Best practice di sicurezza per AWS WAF	29 aprile 2022
AWS Config aggiorna la regola gestita	Con questa versione, AWS Config supporta la regola gestita s3-resources-protected-by-backup-plan.	11 aprile 2022

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono autorizzazioni aggiuntive per ottenere informazioni su tutti gli AWS CloudTrail Event Data Store (EDS) o su uno specifico Event Data Store (EDS), ottenere informazioni su tutte le risorse o su una determinata AWS CloudFormation risorsa, ottenere un elenco di un gruppo di parametri o sottoreti di DynamoDB Accelerator (DAX), ottenere informazioni AWS Database Migration Service sulle AWS DMS() attività di replica per l'account nella regione corrente a cui si accede e ottenere un elenco di tutte le politiche di un tipo specificato. AWS Organizations Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	7 aprile 2022

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • alb-desync-mode-check • autoscaling-capacity-rebalancing • autoscaling-launchconfig-requires-imdsv2 • autoscaling-launch-config-hop-limit • autoscaling-multiple-instance-types • clb-desync-mode-check • ecs-container-insights-enabled • ecs-fargate-latest-platform-version • netfw-policy-default-action-fragment-packets • netfw-policy-default-action-full-packets • netfw-policy-rule-group-associated • redshift-audit-logging-enabled • s3-lifecycle-policy-check • waf-regional-rule-not-empty • waf-regional-rulegroup-not-empty • waf-regional-webacl-not-empty	4 aprile 2022

- vpc-peering-dns-resolution-check

AWS Config Regole di policy personalizzate	Con questa versione, AWS Config consente di creare regole di policy AWS Config personalizzate utilizzando AWS CloudFormation Guard (guard). Guard è un policy-as-code linguaggio che consente di scrivere policy che vengono applicate da AWS Config senza la necessità di creare funzioni Lambda per gestire le regole personalizzate. Le regole scritte utilizzando la policy Guard possono essere create dalla AWS Config console o utilizzando le API delle AWS Config regole. Sono state aggiornate le seguenti pagine della guida per gli sviluppatori: • Regole AWS Config pe rsonalizzate • Creazione di regole AWS Config personalizzate con Guard Sono stati aggiornati i seguenti tipi di dati: • Origine • CustomPolicyDettagli • ConfigRuleEvaluationStatus • GetCustomRulePolicy	4 aprile 2022

	• GetOrganizationCustomRulePolitica • OrganizationCustomPolicyRuleMetadati	
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzarla AWS Config per registrare le modifiche alla configurazione del nuovo tipo di SecurityConfiguration risorsa Amazon EMR. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	31 marzo 2022
AWS Config aggiorna la regola gestita	Con questa versione, AWS Config supporta la regola gestita Virtualmachine-resources-protected-by-backup-plan.	29 marzo 2022

AWS Config Integrazione con Amazon CloudWatch Metrics	Con questa versione, AWS Config ora supporta il monitoraggio dell' AWS Config utilizzo e delle metriche di successo con Amazon CloudWatch nella pagina AWS Config Dashboard. CloudWatch metrics è un servizio di monitoraggio che fornisce dati sulle prestazioni dei sistemi, inclusa la possibili tà di cercare, creare grafici e creare allarmi sulle metriche relative alle risorse. AWS Dalla AWS Config Dashboard , puoi vedere quale traffico sta determinando il tuo AWS Config utilizzo e le metriche chiave per gli errori che si sono verificati nel tuo flusso di lavoro. La pagina seguente è stata aggiornata: • Visualizzazione del pannello di controllo AWS Config	29 marzo 2022
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzarla AWS Config per registrare le modifiche alla configurazione del nuovo tipo di risorsa Amazon GuardDuty Detector. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	24 marzo 2022

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • clb-multiple-az • cloudfront-no-deprecated-ssl-protocols • cloudfront-traffic-to-origin-encrypted • cloudwatch-alarm-action-enabled-check • ec2-no-amazon-key-pair • ec2-paravirtual-instance-check • ec2-token-hop-limit-check • ec2-transit-gateway-auto-vpc-attach-disabled • ecr-private-lifecycle-policy-configured • efs-access-point-enforce-root-directory • efs-access-point-enforce-user-identity • elbv2-multiple-az • kinesis-stream-encrypted • redshift-default-db-name-check • s3-event-notifications-enabled • sns-topic-message-delivery-notification-enabled • waf-global-rulegroup-not-empty	23 marzo 2022

	• waf-global-rule-not-empty	
AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config aggiorna i seguenti pacchetti di conformità: • Best practice operative per CIS Critical Security Controls v8 IG1 • Best practice operative per CIS Critical Security Controls v8 IG2 • Best practice operative per CIS Critical Security Controls v8 IG3 • Best practice operative per AWS Well-Architected Framework Security Pillar • Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello basso • Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello medio • Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello alto • Best practice operative per MAS Notice 655 • Best practice operative per NIST 1800-25	16 marzo 2022

Aggiornamento IAM di sicurezza	La policy `AWSConfigServiceRolePolicy` e la policy `AWS_ConfigRole` ora concedono autorizzazioni aggiuntive per AWS CloudFormation. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	14 marzo 2022
AWS Config aggiorna le regole gestite	Con questa versione, AWS Config aggiorna le seguenti regole gestite: • aurora-resources-protected-by-backup-plan • dynamodb-resources-protected-by-backup-plan • ebs-resources-protected-by-backup-plan • ec2-resources-protected-by-backup-plan • efs-resources-protected-by-backup-plan • fsx-resources-protected-by-backup-plan • rds-resources-protected-by-backup-plan	10 marzo 2022

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzarla AWS Config per registrare le modifiche alla configurazione dei nuovi tipi di risorse pubbliche di Amazon Elastic Container Registry. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	4 marzo 2022
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione di nuovi tipi di risorse Amazon Elastic Compute Cloud. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	28 febbraio 2022
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • codedeploy-auto-rollback-monitor-enabled • codedeploy-ec2-minimum-healthy-hosts-configured • codedeploy-lambda-allatonce-traffic-shift-disabled	25 febbraio 2022

Registrazione e monitoraggio in fase di aggiornamento AWS Config	Con questa versione, AWS Config aggiorna la pagina Monitoring AWS Config with Amazon EventBridge Events per sostituire i riferimenti ad Amazon CloudWatch Events. Amazon EventBridge è il modo preferito per gestire i tuoi eventi. CloudWatch Events e EventBridge 2 sono lo stesso servizio e la stessa API di base, ma EventBridge offrono più funzionalità. Le modifiche apportate in una delle due console CloudWatch o EventBridge verranno visualizz ate in ciascuna console. Per ulteriori informazioni, consulta Amazon. EventBridge	24 febbraio 2022
AWS Pagina SDK per AWS Config	Con questa versione, AWS Config introduce una pagina Utilizzo AWS Config con un AWS SDK. AWS i kit di sviluppo software (SDK) sono disponibili per molti linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice, e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.	24 febbraio 2022

Aggiornamento della policy di attendibilità del ruolo IAM di sicurezza	Con questa versione, AWS Config aggiorna la dichiarazione sulla politica di fiducia di IAM per includere protezioni di sicurezza nella policy di fiducia che limitano l'accesso con `sourceARN` e/o `sourceAccountId` per l'operazione AWS Security Token Service ()AWS STS. Questo aiuta a garantire che la policy di attendibilità del ruolo IAM acceda alle risorse solo per conto degli utenti e degli scenari previsti. La pagina seguente è stata aggiornata: • Aggiunta di una policy di attendibilità IAM al ruolo	18 febbraio 2022

Modifiche alla registrazione dei tipi di risorse globali	AWS Config ora cambia il modo in cui i nuovi tipi di risorse globali vengono registrati in AWS Config Recording. I tipi di risorse globali sono AWS risorse che non richiedono di specifica re una regione al momento della creazione. Prima di questa modifica, era possibile abilitare la registrazione dei tipi di risorse globali in tutte le regioni supportate in AWS Config. Dopo questa modifica, i nuovi tipi di risorse globali inseriti nella AWS Config registrazione possono essere registrati solo nella regione di origine del servizio per la partizione commerciale e AWS GovCloud (Stati Uniti occidentali) per la partizion e. AWS GovCloud (US) Ora sarà possibile visualizzare gli elementi di configura zione per questi nuovi tipi di risorse globali solo nella loro regione di origine e (Stati Uniti occidentali). AWS GovCloud Per un elenco delle regioni di origine dei tipi di risorse globali introdotti dopo febbraio 2022, consulta la tabella nella pagina Registrazione di tutti i tipi di risorse supportati.	18 febbraio 2022

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono l'autorizzazione a ottenere dettagli sugli ambienti Elastic Beanstalk e una descrizione delle impostazioni per il set di configurazione Elastic Beanstalk specificato, ottenere una mappa delle nostre versioni di Elasticsearch, descrivere i gruppi di opzioni OpenSearch di Amazon RDS disponibili per un database e ottenere informazioni su una configurazione di distribuzione. CodeDeploy Questa policy ora concede anche l'autorizzazione a recuperare il contatto alternativo specificato allegato a una Account AWS, recuperare informazioni su una policy, recuperare una AWS Organizations policy del repository Amazon ECR, recuperare informazioni su una AWS Config regola archiviata, recuperare un elenco di famiglie di definizioni di attività Amazon ECS, elencare le unità organizzative (OU) principali o principali dell'unità organizzativa o dell'account figlio specificato ed elencare le politiche	10 febbraio 2022

collegate alla radice, all'unità organizzativa o all'account di destinazione specificati. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • autoscaling-multiple-az • codebuild-project-artifact-encryption • codebuild-project-environment-privileged-check • codebuild-project-logging-enabled • codebuild-project-s3-logs-encrypted • ec2-security-group-attached-to-eni-periodic • ecr-private-image-scanning-enabled • ecr-private-tag-immutability-enabled • ecs-containers-nonprivileged • ecs-containers-readonly-access • ecs-no-environment-secrets • ecs-task-definition-memory-hard-limit • ecs-task-definition-nonroot-user • ecs-task-definition-pid-mode-check • eks-cluster-oldest-supported-version	10 febbraio 2022

	• eks-cluster-supported-version • lambda-vpc-multi-az-check • nacl-no-unrestricted-ssh-rdp • netfw-stateless-rule-group-not-empty • rds-cluster-default-admin-check • rds-db-security-group-not-allowed • rds-instance-default-admin-check • redshift-default-admin-check • s3-bucket-acl-prohibited • s3-version-lifecycle-policy-check • waf-global-webacl-not-empty	
Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono l'autorizzazione a creare gruppi e flussi di CloudWatch log Amazon e a scrivere log su flussi di log creati. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	2 febbraio 2022

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • opensearch-access-control-enabled • opensearch-audit-logging-enabled • opensearch-data-node-fault-tolerance • opensearch-encrypted-at-rest • opensearch-https-required • opensearch-in-vpc-only • opensearch-logs-to-cloudwatch • opensearch-node-to-node-encryption-check	31 gennaio 2022
AWS Config supporta nuovi tipi di risorse	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione dei tipi di AWS CodeDeploy risorse. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	5 gennaio 2022

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzarla AWS Config per registrare le modifiche alla configurazione di nuovi tipi di SageMaker risorse Amazon. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	20 dicembre 2021
AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta i seguenti pacchetti di conformità: • Best practice operative per la guida alla cibersicurezza dell'ENISA per le PMI	20 dicembre 2021
AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta i seguenti pacchetti di conformità: • Best practice operative per NIST 800 172 • Best practice operative per NIST 800 181 È aggiornato il seguente pacchetto di conformità: • Best practice operative per K-ISMS	18 novembre 2021

AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta i seguenti pacchetti di conformità: • Best practice operative per Gateway Amazon API • Best practice operative per AWS Backup • Best practice operative per CISA Cyber Essentials • Migliori pratiche operative per DevOps • Best practice operative per NIST Privacy Framework v1.0 Sono stati aggiornati i seguenti pacchetti di conformità: • Best practice operative per FedRAMP(Low) • Best practice operative per FedRAMP (Moderato)	29 ottobre 2021
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzarla AWS Config per registrare le modifiche alla configurazione di nuovi tipi di risorse Amazon OpenSearch Service. Per ulteriori informazi oni, consulta Tipi di risorsa supportati.	12 ottobre 2021

AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config aggiorna il seguente pacchetto di conformità: • Best practice operative per MAS TRMG	12 ottobre 2021

AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config aggiorna i seguenti pacchetti di conformità: • Best practice operative per ABS CCIG 2.0 Material Workloads • Best practice operative per ABS CCIG 2.0 Standard Workloads • Best practice operative per ACSC Essentials 8 • Best practice operative per ACSC ISM • Best practice operative per BNM RMiT • Best practice operative per CMMC – Livello 1 • Best practice operative per CMMC – Livello 2 • Best practice operative per CMMC – Livello 3 • Best practice operative per CMMC – Livello 4 • Best practice operative per CMMC – Livello 5 • Best practice operative per FDA Titolo 21 CFR Parte 11 • Best practice operative per FFIEC • Best practice operative per MAS Notice 655 • Best practice operative per NBC TRMG	30 settembre 2021

	• Best practice operative per NERC CIP • Best practice operative per NIST 800-53 rev 5	
Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono l'autorizzazione a ottenere dettagli su uno o più domini Amazon OpenSearch OpenSearch Service (Service) e a ottenere un elenco dettagliato dei parametri per un particolare gruppo di parametri DB di Amazon Relational Database Service (Amazon RDS). Questa politica concede anche l'autorizzazione a ottenere dettagli sugli ElastiCache snapshot di Amazon. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	8 settembre 2021
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione di nuovi tipi di risorse Amazon Elastic Compute Cloud. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	7 settembre 2021

AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config aggiorna i seguenti pacchetti di conformità: • Best practice operative per APRA CPG 234 • Migliori pratiche operative per CIS AWS Foundations Benchmark v1.4 Level 1 • Migliori pratiche operative per CIS AWS Foundations Benchmark v1.4 Level 2 • Best practice operative per i principi di sicurezza cloud NCSC • Best practice operative per NCSC Cyber Assessment Framework • Best practice operative per NIST 800 171 • Best practice operative per NIST CSF • Best practice operative per RBI Cyber Security Framework per UCB • Best practice operative per RBI MD-ITF • Best practice operative per NYDFS 23 • Best practice operative per PCI DSS 3.2.1	30 agosto 2021

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • aurora-resources-protected-by-backup-plan • backup-plan-min-frequency-and-min-retention-check • backup-recovery-point-encrypted • backup-recovery-point-manual-deletion-disabled • backup-recovery-point-minimum-retention-check • dynamodb-resources-protected-by-backup-plan • ebs-resources-protected-by-backup-plan • ec2-resources-protected-by-backup-plan • efs-resources-protected-by-backup-plan • fsx-resources-protected-by-backup-plan • rds-resources-protected-by-backup-plan	20 agosto 2021
AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta il seguente pacchetto di conformità: • Best practice operative per NZISM	20 agosto 2021

Aggiornamento della policy Amazon SNS di sicurezza	Con questa versione, AWS Config aggiorna la dichiarazione sulla politica IAM per l'argomento Amazon SNS quando si utilizzano ruoli collegati ai servizi per includere protezioni di sicurezza che limitano l'accesso con `sourceARN` e/o `sourceAccountId` nella policy dell'argomento. Questo aiuta a garantire che Amazon SNS acceda alle risorse solo per conto degli utenti e degli scenari previsti. La pagina seguente è stata aggiornata: • Autorizzazioni per l'argomento Amazon SNS	17 agosto 2021

Aggiornamento della politica di sicurezza AWS Lambda	Con questa versione, AWS Config aggiorna la politica AWS Lambda basata sulle risorse per le regole AWS Config personalizzate per includere protezioni di sicurezza che limitano l'accesso con `sourceARN` e/o `sourceAccountId` nella richiesta di richiamo. Questo aiuta a garantire che l'accesso alle risorse AWS Lambda avvenga solo per conto degli utenti e degli scenari previsti. Sono state aggiornate le seguenti pagine: • AWS::Config::ConfigRule • Sviluppo di una regola personalizzata per AWS Config	12 agosto 2021
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzarla AWS Config per registrare le modifiche alla configurazione dei tipi di risorse Amazon Kinesis. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	6 agosto 2021

AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta il seguente pacchetto di conformità: • Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello alto Sono stati aggiornati i seguenti pacchetti di conformità: • Best practice operative per AWS Well-Architected Framework Reliability Pillar • Best practice operative per AWS Well-Architected Framework Security Pillar • Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello basso • Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello medio • Best practice operative per la sicurezza HIPAA	30 luglio 2021
AWS Lambda Funzioni di esempio per regole personalizzate AWS Config	Con questa versione, AWS Config fornisce funzioni di esempio in Python in Example AWS Lambda Functions for AWS Config Rules (Python).	29 luglio 2021

Aggiornamento IAM di sicurezza	La policy `AWSConfigServiceRolePolicy` e la policy `AWS_ConfigRole` ora concedono l'autorizzazione per elencare i tag per un gruppo di log, elencare i tag per una macchina a stati ed elencare tutte le macchine a stati. Queste policy ora concedono l'autorizzazione per ottenere dettagli su una macchina a stati. Queste policy ora supportano anche autorizzazioni aggiuntive per Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon, Amazon Amazon Simple Notification Service,, e. SageMaker AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	28 luglio 2021

AWS Config supporta nuovi tipi di risorse	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configura zione dei tipi di AWS Backup risorse. Per ulteriori informazi oni, consulta Tipi di risorsa supportati.	14 luglio 2021
AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta i seguenti pacchetti di conformità: • Best practice operative per CIS Critical Security Controls v8 IG1 • Best practice operative per CIS Critical Security Controls v8 IG2 • Best practice operative per CIS Critical Security Controls v8 IG3 • Best practice operative per NIST 1800 25	9 luglio 2021
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • ssm-document-not-public • s3-account-level-public-acc ess-blocks-periodic	25 giugno 2021

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • ec2-instance-multiple-eni-check • elbv2-acm-certificate-required • autoscaling-launch-config-public-ip-disabled	10 giugno 2021

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono il permesso di visualizzare le autorizzazioni di AWS Systems Manager documenti e informazioni su IAM Access Analyzer. Queste policy ora supportano tipi di AWS risorse aggiuntivi per Amazon Kinesis, Amazon, ElastiCache Amazon EMR, Amazon Route 53 e AWS Network Firewall Amazon Relational Database Service (Amazon RDS). Queste modifiche alle autorizza zioni consentono di AWS Config richiamare le API di sola lettura necessarie per supportare questi tipi di risorse. Queste policy ora supportano anche il filtraggio delle funzioni Lambda @Edge per la regola gestita AWS Config lambda-inside-vpc. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	8 giugno 2021

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • elasticsearch-logs-to-cloudwatch • rds-cluster-multi-az-enabled • api-gw-associated-with-waf • iam-policy-no-statements-with-full-access	19 maggio 2021
AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzarla AWS Config per registrare le modifiche alla configurazione dei tipi di risorse Amazon Elastic File System. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	13 maggio 2021

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` policy e la `AWS_ConfigRole` policy ora concedono le autorizzazioni che consentono di AWS Config effettuare chiamate GET di sola lettura ad API Gateway per supportare una regola di configurazione per API Gateway. Queste politiche aggiungono anche autorizzazioni che consentono di AWS Config richiamare le API di sola lettura di Amazon Simple Storage Service (Amazon S3), necessarie per supportare il nuovo tipo di risorsa. `AWS::S3::AccessPoint` Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	10 maggio 2021
AWS Config Regole personalizzate	Sono state aggiornate le seguenti pagine della guida per gli sviluppatori: • Guida introduttiva alle regole personalizzate per AWS Config • Sviluppo di una regola personalizzata per AWS Config	30 aprile 2021

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • aurora-mysql-backtracking-enabled • ec2-instance-profile-attached • ecs-task-definition-user-for-host-mode-check • no-unrestricted-route-to-igw • rds-automatic-minor-version-upgrade-enabled • redshift-enhanced-vpc-routing-enabled	15 aprile 2021

Aggiornamento IAM di sicurezza	La `AWSConfigServiceRolePolicy` politica e la `AWS_ConfigRole` politica ora concedono l'autorizzazione a visualizzare le informazioni su documenti AWS Systems Manager specifici. Queste policy ora supportano anche tipi di AWS risorse aggiuntivi per AWS Backup Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon SageMaker AWS Database Migration Service Kinesis, Amazon e Amazon Route 53. Queste modifiche alle autorizzazioni consentono di AWS Config richiamare le API di sola lettura necessari e per supportare questi tipi di risorse. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Config.	14 aprile 2021

Conformità dei pacchetti di conformità come elementi di configurazione (CI)	In questa versione, AWS Config supporta la conformit à al Conformance Pack come elementi di configurazione. Ciò consente di: • Visualizzare una timeline delle modifiche apportate allo stato di conformità dei pacchetti di conformità • Aggregare la conformità dei pacchetti di conformità su più account e regioni • Utilizzare le query avanzate per verificare la conformità dei pacchetti di conformità Sono stati aggiornati i seguenti tipi di dati: • DescribeAggregateComplianceByConformancePacks • GetAggregateConformancePackComplianceSummary Sono state aggiornate le seguenti pagine della guida per gli sviluppatori: • Visualizzazione dei dati di conformità nel pannello di controllo dei pacchetti di conformità	30 marzo 2021

	• Visualizzazione della timeline della cronologia della conformità dei pacchetti di conformità • Visualizzazione dei dati di conformità e inventario nel pannello di controllo dell'aggregatore • Interrogazione dello stato di configurazione attuale delle risorse AWS • Tipi di risorsa supportati	
Aggiornamento della paginazione	Con questa versione, la funzionalità di interrogazioni AWS Config avanzate ora supporta l'impaginazione per le query che contengono funzioni aggregate, come COUNT e SUM. Ora puoi utilizzare le query avanzate per ottenere risultati completi per le query aggregate tramite la paginazione, in precedenza limitate a 500 righe. Per ulteriori informazioni, vedere Interrogazione dello stato di configurazione corrente delle risorse AWS	26 marzo 2021
Supporto di una regione	Con questa versione, AWS Config and AWS Config Rules è ora supportato nella regione Asia Pacifico (Osaka).	4 marzo 2021

AWS Config supporta nuovi tipi di risorse	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione dei tipi di risorse Amazon Elastic Container Registry, Amazon Elastic Container Service e Amazon Elastic Kubernetes Service. Per ulteriori informazi oni, consulta Tipi di risorsa supportati.	25 febbraio 2021
Supporto per la crittografia KMS	Con questa versione, AWS Config consente di utilizzare la crittografia basata su KMS sugli oggetti distribuiti da AWS Config for S3 bucket Delivery. Sono stati aggiornati i seguenti tipi di dati: • DeliveryChannel • PutDeliveryCanale Sono state aggiornate le seguenti pagine della guida per gli sviluppatori: • Autorizzazioni per la chiave KMS • Autorizzazioni per il ruolo IAM assegnato a AWS Config	16 febbraio 2021

AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • secretsmanager-secret-periodic-rotation • secretsmanager-secret-unused • secretsmanager-using-cmk	16 febbraio 2021
Supporto regionale per la funzionalità di salvataggio delle query	Con questa versione, le interrogazioni salvate sono ora supportate nelle regioni AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali).	15 febbraio 2021
Supporto regionale per l'aggregazione di dati multi-regione multi-account	Con questo rilascio, l'aggregazione di dati multi-regione multi-account è ora supportata nelle regioni Africa (Città del Capo) ed Europa (Milano). Per ulteriori informazioni, consulta Aggregazione di dati multi-regione multi-account.	15 febbraio 2021
Supporto regionale alle query avanzate	Con questo rilascio, le query avanzate sono ora supportate nelle regioni Africa (Città del Capo) ed Europa (Milano). Per ulteriori informazioni, vedere Interrogazione dello stato delle risorse della configurazione corrente. AWS	15 febbraio 2021

AWS Config notifica della cronologia della documentazione disponibile tramite feed RSS	Ora puoi ricevere notifiche sugli aggiornamenti della AWS Config documentazione iscrivendoti a un feed RSS.	1 gennaio 2021

Aggiornamenti precedenti

La tabella seguente descrive la cronologia dei rilasci della documentazione AWS Config precedenti al 31 dicembre 2020.

Modifica	Descrizione	Data di rilascio
Supporto per la funzionalità di salvataggio delle query	Con questa versione, ti AWS Config consente di salvare le tue domande. Dopo aver salvato la query, puoi cercarla, copiarla nell'editor di query, modificarla o eliminarla. Per ulteriori informazioni su come salvare una query, consulta Query con l'editor di query SQL (console) eQuery con l'editor di query SQL (AWS CLI). Per ulteriori informazioni sulle API, consulta la documentazione di riferimento delle API di AWS Config : • PutStoredQuery • GetStoredDomanda • ListStoredInterrogazioni • DeleteStoredQuery Consultare anche Restrizioni dei servizi.	21 dicembre 2020

Modifica	Descrizione	Data di rilascio
Supporto per i controlli di processo	Questa versione AWS Config supporta i controlli di processo, un tipo di AWS Config regola che consente di tenere traccia delle attività esterne e interne che richiedono la verifica nell'ambito dei pacchetti di conformità. Con i controlli di processo, puoi elencare la conformità dei requisiti e delle azioni in un'unica posizione. Per ulteriori informazioni sui controlli di processo, consulta l'AWS Config Controlli di processo all'interno di un pacchetto di conformitàargomento e l'API di PutExternalvalutazione.	17 dicembre 2020

Modifica	Descrizione	Data di rilascio
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • api-gw-ssl-enabled • api-gw-xray-enabled • beanstalk-enhanced-health-reporting-enabled • cloudfront-accesslogs-enabled • cloudfront-associated-with-waf • cloudfront-custom-ssl-certificate • elastic-beanstalk-managed-updates-enabled • rds-cluster-iam-authentication-enabled • redshift-cluster-kms-enabled • s3-bucket-level-public-access-prohibited • subnet-auto-assign-public-ip-disabled • vpc-network-acl-unused-check	17 dicembre 2020
AWS Config supporta AWS Network Firewall	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione dei tuoi AWS Network Firewall FirewallPolicy tipi di risorse e di Firewall. RuleGroup Per ulteriori informazioni, consulta Tipi di risorsa supportati.	4 dicembre 2020

Modifica	Descrizione	Data di rilascio
Aggiornamento della documentazione	AWS Config ha aggiunto il supporto per l'aggregazione dei dati delle risorse a livello di organizzazione in un account amministratore delegato. Adesso puoi utilizzare un account amministratore delegato per aggregare i dati di configurazione e conformità delle risorse provenienti da tutti gli account membri di un'organizzazione in AWS Organizations. Per ulteriori informazioni, consulta Aggregator e. PutConfiguration Impostazione di un aggregatore utilizzando la Console Registrazione di un amministratore delegato	4 dicembre 2020

Modifica	Descrizione	Data di rilascio
AWS Config supporta nuovi pacchetti di conformità	• Best practice operative per CMMC – Livello 3 • Best practice operative per CMMC – Livello 4 • Best practice operative per CMMC – Livello 5 • Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello basso • Best practice operative per Esquema Nacional de Seguridad (ENS) – Livello medio • Best practice operative per NCSC Cyber Assessment Framework • Best practice operative per RBI Cyber Security Framework per UCB	30 ottobre 2020

Modifica	Descrizione	Data di rilascio
AWS Config supporta nuovi pacchetti di conformità	• Best practice operative per ACSC Essentials 8 • Best practice operative per ACSC ISM • Best practice operative per IA e ML • Best practice operative per la gestione degli asset • Best practice operative per BCP e DR • Best practice operative per EC2 • Best practice operative per K-ISMS • Best practice operative per il bilanciamento del carico • Best practice operative per la registrazione • Best practice operative per il monitoraggio • Best practice operative per serverless	22 ottobre 2020

Modifica	Descrizione	Data di rilascio
AWS Config supporta nuovi pacchetti di conformità	• Best practice operative per APRA CPG 234 • Best practice operative per FedRAMP (Low) • Best practice operative per MAS Notice 655 • Best practice operative per NBC TRMG • Best practice operative per i principi di sicurezza cloud NCSC • Best practice operative per RBI MD-ITF	15 ottobre 2020

Modifica	Descrizione	Data di rilascio
AWS Config supporta nuovi pacchetti di conformità	• Best practice operative per ABS CCIG 2.0 Material Workloads • Best practice operative per ABS CCIG 2.0 Standard Workloads • Best practice operative per BNM RMiT • Best practice operative per la resilienza dei dati • Best practice operative per data lake e servizi di analisi • Best practice operative per la crittografia e la gestione delle chiavi • Best practice operative per FDA Titolo 21 CFR Parte 11 • Best practice operative per risorse accessibili pubblicamente • Best practice operative per MAS TRMG • Best practice operative per NERC CIP BCSI • Best practice operative per NYDFS 23	8 ottobre 2020

Modifica	Descrizione	Data di rilascio
AWS Config supporta nuovi pacchetti di conformità	• Best practice operative per AWS Well-Architected Framework Reliability Pillar • Best practice operative per AWS Well-Architected Framework Security Pillar • Best practice operative per CMMC – Livello 1 • Best practice operative per CMMC – Livello 2 • Best practice operative per servizi di calcolo • Best practice operative per servizi di database • Best practice operative per i servizi di gestione e governance • Best practice operative per servizi di rete e distribuzione di contenuti • Best practice operative per servizi di sicurezza, identità e conformità • Best practice operative per servizi di archiviazione	26 ottobre 2020
AWS Config supporta nuovi pacchetti di conformità	• Best practice operative per FedRAMP (Moderato) • Best practice operative per FFIEC • Best practice operative per la sicurezza HIPAA • Best practice operative per NIST 800-53 rev 4 • Best practice operative per NIST 800 171	28 settembre 2020

Modifica	Descrizione	Data di rilascio
Aggiornamento della documentazione	Sono stati aggiornati i seguenti argomenti dei pacchetti di conformità. • Prerequisiti • Distribuzione di un pacchetto di conformità utilizzando la console AWS Config • Gestione dei pacchetti di conformità in tutti gli account dell'organizzazione	28 settembre 2020
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • iam-customer-policy-blocked-kms-actions • iam-inline-policy-blocked-kms-actions	17 settembre 2020
AWS Config supporta AWS WAF v2	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione dei tipi di WebACL, IPSet RegexPatternSet e di risorse AWS WAF v2. RuleGroup ManagedRuleSet Per ulteriori informazioni, consulta Tipi di risorsa supportati.	1 settembre 2020

Modifica	Descrizione	Data di rilascio
Aggiornamento della documentazione	È stata aggiunta una nota a Accesso completo a AWS Config sulla creazione di autorizzazioni personalizzate che garantiscono l'accesso completo. È stata aggiornata la documentazione per le seguenti regole: • s3-bucket-server-side-encryption-enabled • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-platform-check	24 agosto 2020
Aggiornamento della documentazione	Best practice operative per PCI DSS 3.2.1 e i modelli Best practice operative per NIST CSF sono stati aggiornati.	14 agosto 2020
Aggiornamento della documentazione	Sono state aggiunte query su relazioni di esempio. Per ulteriori informazioni, consulta Esempi di query sulle relazioni.	30 luglio 2020

Modifica	Descrizione	Data di rilascio
Aggiornamento della documentazione	Sono stati aggiornati i seguenti tipi di dati: • ConfigurationAggregator • RemediationConfiguration • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStati • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus	23 luglio 2020
AWS Config supporta il tipo di risorsa AWS Systems Manager	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione del tipo di risorsa dati del file AWS Systems Manager. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	9 luglio 2020
Aggiornamento della documentazione	Best practice operative per la gestione delle AWS identità e degli accessi e i modelli Best practice operative per PCI DSS 3.2.1 sono stati aggiornati.	9 luglio 2020

Modifica	Descrizione	Data di rilascio
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • account-part-of-organizations • alb-http-drop-invalid-header-enabled • alb-waf-enabled • cloudfront-default-root-object-configured • cloudfront-origin-access-identity-enabled • cloudfront-origin-failover-enabled • cloudfront-sni-enabled • cloudtrail-security-trail-enabled • cw-loggroup-retention-period-check • dax-encryption-enabled • dynamodb-in-backup-plan • ebs-in-backup-plan • ec2-imdsv2-check • efs-in-backup-plan • eks-endpoint-no-public-access • eks-secrets-encrypted • elasticsearch-node-to-node-encryption-check • elb-cross-zone-load-balancing-enabled • elb-tls-https-listeners-only • iam-no-inline-policy-check • rds-cluster-deletion-protection-enabled	9 luglio 2020

Modifica	Descrizione	Data di rilascio
	• rds-in-backup-plan • rds-instance-deletion-protection-enabled • rds-instance-iam-authentication-enabled • rds-logging-enabled • redshift-backup-enabled • waf-classic-logging-enabled • wafv2-logging-enabled Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	
Supporto regionale per l'aggregazione di dati multi-regione multi-account	Con questo rilascio, l'aggregazione di dati multi-regione multi-account è ora supportata nelle regioni Asia Pacifico (Hong Kong) e Medio Oriente (Bahrein). Per ulteriori informazioni, consulta Multi-Account Multi-Region Data Aggregation e Risoluzione dei problemi per l'aggregazione di dati da più account e regioni.	1 luglio 2020
Supporto regionale alle query avanzate	Con questo rilascio, le query avanzate sono ora supportate nelle regioni Asia Pacifico (Hong Kong) e Medio Oriente (Bahrein). Per ulteriori informazioni, consulta Query dello stato di configurazione corrente delle risorse AWS.	1 luglio 2020

Modifica	Descrizione	Data di rilascio
Aggiornamento della documentazione	È stata aggiornata la documentazione per le seguenti regole: • ec2-managedinstance-association-compliance-status-check • iam-policy-no-statements-with-admin-access • required-tags • restricted-common-ports • rds-snapshots-public-prohibited • s3-bucket-policy-grantee-check	30 giugno 2020
Aggiornamento della documentazione	La documentazione è stata aggiornata con informazioni sulla sicurezza per AWS Config. Per informazioni, consulta Sicurezza in AWS Config.	24 giugno 2020
Aggiornamento della documentazione	AWS Control Tower Il modello Detective Guardrails Conformance Pack è stato aggiornato. Per ulteriori informazioni, consulta AWSPacchetto di conformità Control Tower Detective Guardrails.	4 giugno 2020
AWS Config supporta un nuovo pacchetto di conformità	Con questa versione, AWS Config supporta il pacchetto di conformità Operational Best Practices for NIST CSF. Per ulteriori informazioni, consulta Best practice operative per NIST CSF .	29 maggio 2020

Modifica	Descrizione	Data di rilascio
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • dynamodb-pitr-enabled • dynamodb-table-encrypted-kms • ec2-ebs-encryption-by-default • rds-snapshot-encrypted • redshift-require-tls-ssl • s3-bucket-default-lock-enabled • s3-default-encryption-kms • securityhub-enabled • sns-encrypted-kms Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	28 maggio 2020

Modifica	Descrizione	Data di rilascio
Supporto per amministratore delegato	Con questa versione, è possibile distribuire AWS Config regole e pacchetti di conformità da qualsiasi account membro delegato dell'organizzazione, oltre all'account di gestione. Per ulteriori informazioni sulle API, consulta la documentazione di riferimento delle API di AWS Config : • PutOrganizationConfigRule • PutOrganizationConformancePack • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStati • DeleteOrganizationConfigRule • DeleteOrganizationConformancePack • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus Per ulteriori informazioni, consulta Restrizioni dei servizi.	27 maggio 2020

Modifica	Descrizione	Data di rilascio
AWS Config regole Region support	Con questa versione, poche AWS Config regole sono supportate nelle regioni di Africa (Città del Capo) ed Europa (Milano). Per un elenco dettagliato delle regole e delle regioni in cui sono supportate, vedere Elenco di regole AWS Config gestite.	28 aprile 2020
AWS Config supporta nuovi pacchetti di conformità	Con questa versione, AWS Config supporta due pacchetti di conformità. • AWS Pacchetto di conformità Control Tower Detective Guardrails • Best practice operative per PCI-DSS Per ulteriori informazioni, consulta Modelli di esempio di pacchetto di conformità.	22 aprile 2020
AWS Config supporta AWS Secrets Manager	Con questa versione, è possibile utilizzare AWS Config per registrar e le modifiche alla configurazione del segreto di Secrets Manager. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	20 aprile 2020

Modifica	Descrizione	Data di rilascio
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • secretsmanager-rotation-enabled-check • secretsmanager-scheduled-rotation-success-check Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	16 aprile 2020
Supporto regionale del pacchetto di conformità	Con questo rilascio, i pacchetti di conformità sono ora supportati nelle regioni Asia Pacifico (Hong Kong) e Medio Oriente (Bahrein). Per ulteriori informazioni, consulta Conformance Packs.	8 aprile 2020
Aggiornamento della documentazione	AWS Config i limiti sono disponibili in questa guida per sviluppatori. Per ulteriori informazioni, consulta Restrizioni dei servizi.	8 aprile 2020
Aggiornamento della documentazione	Le risorse di terze parti gestite (ovvero create/aggiornate/eliminate) tramite il AWS CloudFormation registro vengono automaticamente registrate come elementi di configurazione. AWS Config Per ulteriori informazioni, consulta Registrazione delle configurazioni per le risorse di terze parti.	30 marzo 2020

Modifica	Descrizione	Data di rilascio
Aggiornamento della documentazione	Le regole AWS Config gestite vengono aggiornate per includere informazioni. Regione AWS Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	27 marzo 2020
AWS Config supporta il tipo di risorsa Amazon SNS	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione del tuo argomento Amazon SNS. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	6 marzo 2020
Supporto regionale per l'aggregazione di dati multi-regione multi-account	Con questa release l'aggregazione di dati da più account e regioni è supportata in sei nuove regioni. Per ulteriori informazioni, consulta Multi-Account Multi-Region Data Aggregation.	5 marzo 2020
Supporto regionale alle query avanzate	Con questa versione, le query avanzate sono ora supportate nella regione Europa (Stoccolma). Per ulteriori informazioni, consulta Query dello stato di configurazione corrente delle risorse AWS.	5 marzo 2020

Modifica	Descrizione	Data di rilascio
AWS Config ti consente di eseguire query avanzate con aggregatori di configurazione	Con questa versione, AWS Config aggiunge il supporto per l'esecuzione di query avanzate basate sulle proprietà di configurazione delle risorse con aggregatori di configurazione, consentendo di eseguire le stesse query su più account e regioni. Per ulteriori informazioni, consulta Query dello stato di configurazione corrente delle risorse AWS. Con questa versione, AWS Config aggiunge l'API. `SelectAggregateResourceConfig` Per ulteriori informazioni, SelectAggregateResourceConfigconsulta l'AWS Config API Reference:	28 febbraio 2020
AWS Config supporta il tipo di risorsa Amazon SQS	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione della tua coda Amazon SQS. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	13 febbraio 2020

Modifica	Descrizione	Data di rilascio
AWS CloudFormation supporto per i pacchetti Conformance	Con questa versione, è stato aggiunto il AWS CloudFormation supporto per le seguenti risorse: `AWS::Config::ConformancePack` e `OrganizationConformancePack` • AWS::Config::ConformancePack Utilizza la `AWS::Config::ConformancePack` risorsa per creare un Conformance Pack, ovvero una raccolta di AWS Config regole che possono essere facilmente implementate in un account, in una regione e in tutta l'organizzazione. AWS • AWS::Config::OrganizationConformancePacchetto Utilizza la `AWS::Config::OrganizationConformancePack` risorsa per creare un Organization Conformance Pack contenente informazioni su pacchetti di conformità AWS Config creati negli account dei membri.	13 febbraio 2020

Modifica	Descrizione	Data di rilascio
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • api-gw-execution-logging-enabled • ec2-stopped-instance • elasticache-redis-cluster-automatic-backup-check • emr-master-no-public-ip • guardduty-non-archived-findings • rds-enhanced-monitoring-enabled • s3-account-level-public-access-blocks • sagemaker-endpoint-configuration-kms-key-configured • service-vpc-endpoint-enabled Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	20 dicembre 2019

Modifica	Descrizione	Data di rilascio
Registrazione delle configura zioni per i tipi di risorse personali zzate	Con questa versione, AWS Config introduce il supporto per le configura zioni di registrazione per tipi di risorse personalizzati. È possibile pubblicare i dati di configurazione di risorse di terze parti AWS Config e visualizzare e monitorare l'inventa rio delle risorse e la cronologia di configurazione utilizzando AWS Config console e API. Per ulteriori informazioni, consulta Registrazione delle configurazioni per le risorse di terze parti. Per ulteriori informazioni sulle API, consulta la documentazione di riferimento delle API di AWS Config : • DeleteResourceConfig • PutResourceConfig	20 novembre 2019

Modifica	Descrizione	Data di rilascio
Pacchetti di conformità	Con questa versione, AWS Config introduce i pacchetti di conformità. I pacchetti di conformità consenton o di raggruppare una raccolta di AWS Config regole e azioni correttiv e che possono poi essere implement ate insieme come un'unica entità in un'intera organizzazione. AWS Per ulteriori informazioni, consulta Conformance Packs. Per ulteriori informazioni sulle API, consulta la documentazione di riferimento delle API di AWS Config : • DeleteOrganizationConforman cePack • DeleteOrganizationConforman cePack • DescribeConformancePacchetti • DescribeConformancePacchetti • DescribeConformancePackStatus • DescribeOrganizationConform ancePacks • DescribeOrganizationConform ancePackStatuses • GetConformancePackComplianc eDettagli • GetConformancePackComplianc eRiepilogo • GetOrganizationConformanceP ackDetailedStatus, • PutConformanceConfezione	19 novembre 2019

Modifica	Descrizione	Data di rilascio
	• PutOrganizationConformancePack	
AWS Config supporta Amazon OpenSearch Service e tipi di AWS Key Management Service risorse	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione del tuo dominio e della tua AWS Key Management Service chiave Amazon OpenSearch Service. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	11 novembre 2019
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • dms-replication-not-public • emr-kerberos-enabled • internet-gateway-authorized-vpc-only • kms-cmk-not-scheduled-for-deletion • sagemaker-notebook-no-direct-internet-access • sagemaker-notebook-instance-kms-key-configured • shield-drt-access Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	10 ottobre 2019

Modifica	Descrizione	Data di rilascio
AWS Config supporta il tipo di risorsa Amazon RDS	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione di DBCluster e DB di Amazon Relational Database Service (Amazon RDS). ClusterSnapshot Per ulteriori informazioni, consulta Tipi di risorsa supportati.	17 settembre 2019
AWS Config supporta il tipo di risorsa Amazon QLDB	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione del tipo di risorsa di registro Amazon Quantum Ledger Database (QLDB). Per ulteriori informazioni, consulta Tipi di risorsa supportati.	10 settembre 2019

Modifica	Descrizione	Data di rilascio
AWS Config consente di applicare la riparazione automatic a su risorse non conformi secondo quanto valutato da Rules AWS Config	Con questa versione, AWS Config introduce il supporto per applicare la riparazione automatica utilizzando documenti di AWS Systems Manager automazione su risorse non conformi valutate da Rules. AWS Config Per ulteriori informazioni, consulta Correzione delle risorse non conformi con regole AWS Config. Con questa versione, AWS Config aggiunge le seguenti nuove API. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API AWS Config : • PutRemediationEccezioni • DescribeRemediationEccezioni • DeleteRemediationEccezioni	5 settembre 2019

Modifica	Descrizione	Data di rilascio
AWS Config aggiorna le regole gestite	In questa versione, AWS Config supporta le seguenti regole gestite: • alb-http-to-https-redirection-check • api-gw-cache-enabled-and-encrypted • api-gw-endpoint-type-check • cloudtrail-s3-dataevents-enabled • cloudwatch-log-group-encrypted • ebs-snapshot-public-restorable-check • elb-deletion-protection-enabled • lambda-concurrency-check • lambda-dlq-check • lambda-inside-vpc • shield-advanced-enabled-autorenew • vpc-vpn-2-tunnels-up Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	22 agosto 2019

Modifica	Descrizione	Data di rilascio
AWS Config aggiorna le regole gestite	Con questa versione, AWS Config aggiorna le seguenti regole gestite: • cloudfront-viewer-policy-https • ec2-instance-no-public-ip • ec2-security-group-attached-to-eni • efs-encrypted-check • elasticsearch-encrypted-at-rest • elasticsearch-in-vpc-only • redshift-cluster-public-access-check • vpc-sg-open-only-to-authorized-ports Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	31 luglio 2019
AWS Config supporta i tipi di risorse Amazon EC2	Con questa versione, puoi utilizzar e AWS Config per registrare le modifiche alla configurazione delle seguenti risorse Amazon EC2: VPCendpoint, VPC e VPCEndpoi ntService. PeeringConnection Per ulteriori informazioni, consulta Tipi di risorsa supportati.	12 luglio 2019

Modifica	Descrizione	Data di rilascio
AWS Config consente di gestire le regole all'interno di un'organizzazione AWS Config Account AWS	Con questa versione, AWS Config introduce il supporto per la gestione delle AWS Config regole Account AWS in tutta l'organizzazione. È possibile creare, aggiornare ed eliminare centralmente AWS Config le regole per tutti gli account dell'organizzazione. Per ulteriori informazioni, consulta Gestione AWS Config delle regole per tutti gli account dell'organizzazione. Per ulteriori informazioni sulle API, consulta la documentazione di riferimento delle API di AWS Config : • PutOrganizationConfigRule • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStati • DeleteOrganizationConfigRule	9 luglio 2019
AWS Config supporta i tipi di risorse Amazon S3 e Amazon EC2	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione della AccountPublicAccessBlock risorsa Amazon S3 e alle seguenti risorse Amazon EC2 NatGateway; EgressOnlyInternetGateway, e. FlowLog Per ulteriori informazioni, consulta Tipi di risorsa supportati.	17 maggio 2019

Modifica	Descrizione	Data di rilascio
AWS Config aggiorna le regole gestite	Con questa versione, AWS Config aggiorna le seguenti regole gestite: • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	7 maggio 2019
AWS Config consente di eliminare un'azione di riparazione utilizzando AWS Management Console.	Con questa versione, AWS Config introduce il supporto per eliminare un'azione di riparazione utilizzan do. AWS Management Console Per ulteriori informazioni, consulta Correzione delle risorse non conformi con regole AWS Config.	24 aprile 2019
AWS Config supporta nuove regole gestite	Questa versione supporta una nuova regola gestita: fms-shield-resource-policy-check. Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	7 aprile 2019

Modifica	Descrizione	Data di rilascio
AWS Config supporta il tipo di risorsa Amazon API Gateway	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione delle seguenti risorse di Amazon API Gateway: Api (WebSocket API), RestApi (API REST), Stage (fase WebSocket API) e Stage (fase API REST). Per ulteriori informazioni, consulta Tipi di risorsa supportati.	20 marzo 2019
AWS Config ti consente di eseguire query avanzate	Con questa versione, AWS Config aggiunge il supporto per l'esecuzione di query avanzate basate sulle proprietà di configurazione delle risorse. Per ulteriori informazioni, consulta Query dello stato di configurazione corrente delle risorse AWS. Con questa versione, AWS Config aggiunge l'`SelectResourceConfig` API. Per ulteriori informazioni, consulta SelectResourceConfig nell'AWS Config API Reference:	19 marzo 2019

Modifica	Descrizione	Data di rilascio
AWS Config ti permette di assegnare tag alle tue risorse AWS Config	Con questa versione, AWS Config introduce il supporto per il controllo degli accessi basato su tag per tre AWS Config risorse: `ConfigRule`, `ConfigurationAggregator`, e. `AggregationAuthorization` Per ulteriori informazioni, consulta Tagging delle risorse AWS Config. Con questo rilascio, puoi aggiungere, rimuovere o elencare i tag dalle risorse AWS Config utilizzando le seguenti tipi di dati. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API AWS Config : • ListTagsForResource • TagResource • UntagResource	14 marzo 2019

Modifica	Descrizione	Data di rilascio
AWS Config consente di applicare la correzione alle risorse non conformi, secondo quanto valutato dalle Regole AWS Config	Con questa versione, AWS Config introduce il supporto per applicare la correzione utilizzando documenti di AWS Systems Manager automazione su risorse non conformi valutate da Rules. AWS Config Per ulteriori informazioni, consulta Correzione delle risorse non conformi con regole AWS Config. Con questa versione, AWS Config aggiunge le seguenti nuove API. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API AWS Config : • DeleteRemediationConfigurazione • DescribeRemediationConfigurazioni • DescribeRemediationExecutionStatus • PutRemediationConfigurazioni • StartRemediationEsecuzione	12 marzo 2019

Modifica	Descrizione	Data di rilascio
AWS Config supporta AWS Config le regole nella regione Cina (Ningxia)	Questa versione supporta solo 54 AWS Config regole nella regione Cina (Ningxia). Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite. Tuttavia, attualmente AWS Config non supporta le seguenti regole nella regione Cina (Ningxia): • acm-certificate-expiration-check • cmk-backing-key-rotation-enabled • cloudformation-stack-drift-detection-check • cloudformation-stack-notification-check • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check • dynamodb-table-encryption-enabled • elb-acm-certificate-required • encrypted-volumes • fms-webacl-resource-policy-check	12 marzo 2019

Modifica	Descrizione	Data di rilascio
	• fms-webacl-rulegroup-association-check • guardduty-enabled-centralized • lambda-function-public-access-prohibited • lambda-function-settings-check • rds-storage-encrypted • root-account-mfa-hardware-mfa-enabled • root-account-mfa-enabled • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-grantee-check • s3-bucket-policy-not-more-p ermissive • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited • S3-bucket-server-side-encryption-enabled • s3-bucket-ssl-requests-only	
AWS Config supporta nuove regole gestite	Questa versione supporta le seguenti nuove regole gestite: • iam-user-mfa-enabled • s3-bucket-policy-grantee-check Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	21 gennaio 2019

Modifica	Descrizione	Data di rilascio
AWS Config supporta il tipo di risorsa Service Catalog	Con questa versione, è possibile utilizzare AWS Config per registrar e le modifiche alla configurazione delle seguenti risorse del Service Catalog: CloudFromation prodotto, prodotto fornito e portafoglio. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	11 gennaio 2019
Supporto alle regole collegate ai servizi AWS Config	Con questa versione, AWS Config aggiunge una nuova regola di configurazione gestita che supporta altri AWS servizi per la creazione di AWS Config regole nel tuo account. Per ulteriori informazioni, consulta Regole collegate ai servizi AWS Config.	20 novembre 2018

Modifica	Descrizione	Data di rilascio
AWS Config consente di aggregare i dati di configurazione delle risorse AWS	Con questa versione, AWS Config introduce il supporto per l'aggrega zione dei dati di configurazione delle risorse. AWS Per ulteriori informazi oni, consulta Visualizzazione dei dati di conformità e inventario nel pannello di controllo dell'aggregatore. Con questa versione, AWS Config aggiunge le seguenti nuove API. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API AWS Config : • BatchGetAggregateResourceConfig • GetAggregateDiscoveredResourceConta • GetAggregateResourceConfig • ListAggregateDiscoveredResources	19 novembre 2018
AWS Config supporta nuove regole gestite	Questa versione supporta le seguenti nuove regole gestite: • cloudformation-stack-drift-detection-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	19 novembre 2018

Modifica	Descrizione	Data di rilascio
AWS Config supporta nuove regole gestite	Questa versione supporta le seguenti nuove regole gestite: • access-keys-rotated • cloud-trail-cloud-watch-logs-enabled • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • cmk-backing-key-rotation-enabled • iam-policy-no-statements-with-admin-access • iam-role-managed-policy-check • iam-root-access-key-check • iam-user-unused-credentials-check • mfa-enabled-for-iam-console-access • multi-region-cloudtrail-enabled • root-account-hardware-mfa-enabled • vpc-flow-logs-enabled Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	12 novembre 2018

Modifica	Descrizione	Data di rilascio
AWS Config supporta nuove regole gestite	Questa versione supporta le seguenti nuove regole gestite: • dynamodb-table-encryption-enabled • elb-logging-enabled • rds-instance-public-access-check • vpc-default-security-group-closed Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	24 ottobre 2018
Supporto della cronologia di conformità	Con questa versione, AWS Config ora supporta l'archiviazione della cronologia di conformità delle risorse valutata da AWS Config Rules. Per ulteriori informazioni, consulta Visualizzazione della cronologia di conformità per le risorse.	18 ottobre 2018
Supporto regionale per l'aggregazione di dati da più account e regioni	Con questa release l'aggregazione di dati da più account e regioni è supportata in sei nuove regioni. Per ulteriori informazioni, consulta Multi-Account Multi-Region Data Aggregation.	4 ottobre 2018

Modifica	Descrizione	Data di rilascio
AWS Config supporta le autorizzazioni a livello di risorsa per le azioni delle API di Rules AWS Config	Con questa versione, AWS Config supporta le autorizzazioni a livello di risorsa per determinate azioni dell'API Rules. AWS Config Per ulteriori informazioni sulle API supportate, consulta Autorizzazioni supportate a livello di risorsa per le azioni dell'API Rule AWS Config.	1 ottobre 2018
AWS Config supporta il tipo di risorsa CodePipeline	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione del tipo di AWS CodePipeline risorsa. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	12 settembre 2018

Modifica	Descrizione	Data di rilascio
AWS Config supporta nuove regole gestite	Questa versione supporta le seguenti nuove regole gestite: • ec2-instance-managed-by-systems-manager • ec2-managedinstance-association-compliance-status-check • ec2-managedinstance-patch-compliance-status-check • guardduty-enabled-centralized • rds-snapshots-public-prohibited • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-not-more-permissive Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	5 settembre 2018
AWS Config supporta il tipo di risorsa AWS Systems Manager	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione dei tipi di risorse relative alla conformità delle patch di AWS Systems Manager e alla conformità delle associazioni. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	9 agosto 2018

Modifica	Descrizione	Data di rilascio
AWS Config consente di eliminare i AWS Config dati utilizzando AWS Management Console	Con questa versione, AWS Config introduce il supporto per l'utilizzo AWS Management Console del periodo di conservazione. Nel AWS Management Console, puoi selezionare un periodo di conservazione dei dati personalizzato per il tuo`ConfigurationItems`. Per ulteriori informazioni, consulta Eliminazione dei dati AWS Config.	7 agosto 2018
AWS Config supporta il tipo di AWS Shield risorsa	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione del tipo di risorsa AWS Shield Protection. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	7 agosto 2018
AWS Config supporta AWS PrivateLink	Con questa versione, AWS Config supporta AWS PrivateLink, ti consente di instradare i dati tra Amazon Virtual Private Cloud (VPC) e AWS Config interamente all'interno della rete. AWS Per ulteriori informazioni, consulta Utilizzo AWS Config con l'interfaccia Amazon VPC Endpoints.	31 luglio 2018

Modifica	Descrizione	Data di rilascio
AWS Config ti consente di eliminare i tuoi AWS Config dati	Con questa versione, AWS Config introduce il supporto per il periodo di conservazione. AWS Config ti consente di eliminare i tuoi dati specificando un periodo di conservazione per il tuo `ConfigurationItems` Per ulteriori informazioni, consulta Eliminazione dei dati AWS Config. Con questa versione, AWS Config aggiunge le seguenti nuove API. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API AWS Config : • PutRetentionConfigurazione • DescribeRetentionConfigurazioni • DeleteRetentionConfigurazione	25 maggio 2018
AWS Config supporta nuove regole gestite	Questa versione supporta due nuove regole gestite: • lambda-function-settings-check • s3-bucket-replication-enabled • iam-policy-blacklisted-check Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	10 maggio 2018

Modifica	Descrizione	Data di rilascio
AWS Config supporta il tipo di AWS X-Ray risorsa	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione del tipo di AWS X-Ray EncryptionConfig risorsa. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	1 maggio 2018
AWS Config supporta il tipo di AWS Lambda risorsa e una nuova regola gestita	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione del tipo di risorsa della AWS Lambda funzione. Per ulteriori informazioni, consulta Tipi di risorsa supportati. Questa versione supporta anche la regola gestita lambda-function-public-access-prohibited. Per ulteriori informazioni, consulta AWS Config Regole gestite.	25 aprile 2018
AWS Config supporta il tipo di AWS Elastic Beanstalk risorsa	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione delle risorse dell' AWS Elastic Beanstalk applicazione, della versione dell'applicazione e dell'ambiente. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	24 Aprile 2018

Modifica	Descrizione	Data di rilascio
AWS Config supporta nuove regole gestite	Questa versione supporta due nuove regole gestite: • fms-webacl-resource-policy-check • fms-webacl-rulegroup-association-check Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	4 aprile 2018

Modifica	Descrizione	Data di rilascio
Aggregazione di dati da più account e regioni	Con questa versione, AWS Config introduce l'aggregazione di dati multiaccount e più regioni. Questa funzionalità consente di aggregare AWS Config i dati provenienti da più account o da un'organizzazione e da più regioni in un account aggregato re. Per ulteriori informazioni, consulta Multi-Account Multi-Region Data Aggregation. Con questa versione, AWS Config aggiunge le seguenti nuove API. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API AWS Config : • PutConfigurationAggregatore • DescribePendingAggregationRequests • DeletePendingAggregationRequest • PutAggregationAutorizzazione • DescribeAggregationAutorizzazioni • GetAggregateConfigRuleComplianceSummary • DescribeAggregateComplianceByConfigRules • GetAggregateComplianceDetailsByConfigRegola • DescribeConfigurationAggregatori • DescribeConfigurationAggregatorSourcesStato • DeleteAggregationAutorizzazione	4 aprile 2018

Modifica	Descrizione	Data di rilascio
	• DeleteConfigurationAggregatore	
Monitoraggio AWS Config con Amazon CloudWatch Events	Con questa versione, usa Amazon CloudWatch Events per rilevare e reagire ai cambiamenti nello stato degli AWS Config eventi. Per ulteriori informazioni, consulta Monitoraggio AWS Config con Amazon EventBridge.	29 marzo 2018
Nuova operazione API	Con questa versione, AWS Config aggiunge il supporto per BatchGetResourceConfigl'API, che consente di recuperare in batch lo stato attuale di una o più risorse.	20 marzo 2018
AWS Config supporta il tipo di risorsa AWS WAF RuleGroup	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione delle risorse AWS WAF RuleGroup e AWS WAF RuleGroup Regional. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	15 febbraio 2018

Modifica	Descrizione	Data di rilascio
AWS Config supporta nuove regole gestite	Questa versione supporta le seguenti nuove regole gestite: • elb-acm-certificate-required • elb-custom-security-policy-ssl-check • elb-predefined-security-policy-ssl-check • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • iam-group-has-users-check • s3-bucket-server-side-encryption-enabled Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	25 gennaio 2018
AWS Config supporta il tipo di risorsa Elastic Load Balancing	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione dei sistemi di bilanciamento del carico classici Elastic Load Balancing. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	17 Novembre 2017

Modifica	Descrizione	Data di rilascio
AWS Config supporta Amazon CloudFront e il tipo di AWS WAF risorsa	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione della tua CloudFront distribuzione e della distribuzione in streaming. Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione alle seguenti risorse AWS WAF e alle risorse AWS WAF regionali: regola basata sulla frequenza, regola e ACL Web. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	15 novembre 2017
AWS Config supporta il tipo di AWS CodeBuild risorsa	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione AWS CodeBuild dei tuoi progetti. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	20 ottobre 2017

Modifica	Descrizione	Data di rilascio
AWS Config supporta le risorse di Auto Scaling e una nuova regola gestita	Con questa versione, è possibile utilizzare AWS Config per registrar e le modifiche alla configurazione delle seguenti risorse di Auto Scaling: gruppi, configurazione di avvio, azioni pianificate e policy di scalabilità. Per ulteriori informazioni, consulta Tipi di risorsa supportati. Questa versione supporta anche la seguente regola gestita: • autoscaling-group-elb-healthcheck-required Per ulteriori informazioni, consultare AWS Config Regole gestite.	18 settembre 2017
AWS Config supporta il tipo di risorsa AWS CodeBuild	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione AWS CodeBuild dei tuoi progetti. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	20 ottobre 2017

Modifica	Descrizione	Data di rilascio
AWS Config supporta le risorse di Auto Scaling e una nuova regola gestita	Con questa versione, è possibile utilizzare AWS Config per registrar e le modifiche alla configurazione delle seguenti risorse di Auto Scaling: gruppi, configurazione di avvio, azioni pianificate e policy di scalabilità. Per ulteriori informazioni, consulta Tipi di risorsa supportati. Questa versione supporta anche la seguente regola gestita: • autoscaling-group-elb-healthcheck-required Per ulteriori informazioni, consultare AWS Config Regole gestite.	18 settembre 2017
AWS Config supporta il tipo di risorsa della tabella DynamoDB e una nuova regola gestita	Con questa versione, è possibile utilizzare AWS Config per registrare le modifiche alla configurazione delle tabelle DynamoDB. Per ulteriori informazioni, consulta Tipi di risorsa supportati. Questa versione supporta la seguente regola gestita: • dynamodb-autoscaling-enabled Per ulteriori informazioni, consulta AWS Config Regole gestite.	8 settembre 2017

Modifica	Descrizione	Data di rilascio
AWS Config supporta due nuove regole gestite per Amazon S3	Questa versione supporta due nuove regole gestite: • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited Per ulteriori informazioni, consulta AWS Config Regole gestite.	14 agosto 2017
Nuova pagina nella console AWS Config	Puoi utilizzare la Dashboard nella AWS Config console per visualizzare quanto segue: • Numero totale di risorse • Numero totale di regole • Numero di risorse non conformi • Numero di regole non conformi Per ulteriori informazioni, consulta Visualizzazione del AWS Config pannello di controllo.	17 luglio 2017
Nuova operazione API	È possibile utilizzare l'GetDiscoveredResourceCountsoperazione per restituire il numero di tipi di risorse, il numero di ciascun tipo di risorsa e il numero totale di risorse registrate AWS Config in una regione per la propria Account AWS.	17 luglio 2017

Modifica	Descrizione	Data di rilascio
AWS Config supporta il tipo di risorsa AWS CloudFormation stack e una nuova regola gestita	Con questa versione, è possibile utilizzarla AWS Config per registrare le modifiche alla configurazione degli AWS CloudFormation stack. Per ulteriori informazioni, consulta Tipi di risorsa supportati. Questa versione supporta la seguente regola gestita: • cloudformation-stack-notification-check Per ulteriori informazioni, consulta AWS Config Regole gestite.	6 luglio 2017
Contenuti nuovi e aggiornati	Questa versione aggiunge il supporto per AWS Config le regole nella regione Canada (Centrale) e Sud America (San Paolo). Per tutte le aree che supportano le regole di configurazione AWS Config e, vedere Regioni AWS ed Endpoints in. Riferimenti generali di AWS	5 luglio 2017

Modifica	Descrizione	Data di rilascio
Contenuti nuovi e aggiornati	AWS Config Le regole sono disponibili nella regione. AWS GovCloud (US) Per ulteriori informazioni, consulta la Guida per l'utente AWS GovCloud (US). Per le aree che supportano AWS Config, vedi Regioni AWS ed Endpoints in. Riferimenti generali di AWS	8 giugno 2017
AWS Config supporta il tipo di risorsa Amazon CloudWatch Alarm e tre nuove regole gestite	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione dei tuoi CloudWatch allarmi Amazon. Per ulteriori informazioni, consulta Tipi di risorsa supportati. Questa versione supporta tre nuove regole gestite: • cloudwatch-alarm-action-check • cloudwatch-alarm-resource-check • cloudwatch-alarm-settings-check Per ulteriori informazioni, consulta AWS Config Regole gestite.	1 giugno 2017

Modifica	Descrizione	Data di rilascio
Contenuti nuovi e aggiornati	Questa versione supporta la specifica del numero di versione dell'applicazione per le seguenti regole gestite: • ec2-managedinstance-applications-blacklisted • ec2-managedinstance-applications-required Per ulteriori informazioni, consulta AWS Config Regole gestite.	1 giugno 2017
Contenuti nuovi e aggiornati	Questa versione aggiunge il supporto per AWS Config le regole nella regione Asia Pacifico (Mumbai). Per ulteriori informazioni, consulta Regioni AWS ed endpoint nella Riferimenti generali di AWS.	27 Aprile 2017

Modifica	Descrizione	Data di rilascio
Contenuti nuovi e aggiornati	Questa versione aggiorna la console e consente per la prima volta di aggiungere regole gestite di AWS Config al tuo account. Quando configuri AWS Config le regole per la prima volta o in una nuova regione, puoi cercare le regole AWS gestite per nome, descrizione o etichetta. Puoi scegliere Seleziona tutto per selezionare tutte le regole oppure Cancella tutto per cancellare tutte le regole. Per ulteriori informazioni, consulta Aggiunta, visualizzazione, aggiornamento ed eliminazione delle regole (console).	5 Aprile 2017
AWS Config supporta nuove regole gestite	Questa versione supporta le seguenti nuove regole gestite: • acm-certificate-expiration-check • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-inventory-blacklisted • ec2-volume-inuse-check • iam-user-group-membership-check • iam-user-no-policies-check • s3-bucket-ssl-requests-only Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	21 febbraio 2017

Modifica	Descrizione	Data di rilascio
Contenuti nuovi e aggiornati	Questa versione aggiunge il supporto per AWS Config le regole nella regione Europa (Londra). Per ulteriori informazioni, consulta Regioni AWS ed endpoint nella Riferimenti generali di AWS.	21 febbraio 2017
Contenuti nuovi e aggiornati	Questa versione aggiunge AWS CloudFormation modelli per le regole AWS Config gestite. Puoi utilizzare i modelli per creare regole gestite per il tuo account. Per ulteriori informazioni, consulta Creazione di regole gestite di AWS Config con modelli AWS CloudFormation.	16 febbraio 2017
Contenuti nuovi e aggiornati	Questa versione aggiunge il supporto per una nuova modalità di prova per l'API `PutEvaluations` . Nella regola personalizzata, imposta il parametro `TestMode` su "true" per verificare se la funzione AWS Lambda consegna i risultati di valutazione a AWS Config. Le valutazioni esistenti non vengono aggiornate e i risultati non vengono inviati a AWS Config. Per ulteriori informazioni, PutEvaluationsconsulta l'AWS Config API Reference.	16 febbraio 2017

Modifica	Descrizione	Data di rilascio
Contenuti nuovi e aggiornati	Questa versione aggiunge il supporto per AWS Config le regole nelle regioni Asia Pacifico (Seoul) e Stati Uniti occidentali (California settentri onale). Per ulteriori informazioni, consulta Regioni AWS ed endpoint nella Riferimenti generali di AWS.	21 dicembre 2016
Contenuti nuovi e aggiornati	Questa versione aggiunge il supporto per la AWS Config regione Europa (Londra). Per ulteriori informazioni, consulta Regioni AWS ed endpoint nella Riferimenti generali di AWS.	13 dicembre 2016
Contenuti nuovi e aggiornati	Questa versione aggiunge il supporto per AWS Config la regione Canada (Centrale). Per ulteriori informazioni, consulta Regioni AWS ed endpoint nella Riferimenti generali di AWS.	8 dicembre 2016

Modifica	Descrizione	Data di rilascio
AWS Config supporta i tipi di risorse Amazon Redshift e due nuove regole gestite	Con questa versione, puoi utilizzare AWS Config per registrare le modifiche alla configurazione dei cluster Amazon Redshift, dei gruppi di parametri del cluster, dei gruppi di sicurezza del cluster, degli snapshot dei cluster, dei gruppi di sottoreti del cluster e degli abbonamenti a eventi. Per ulteriori informazioni, consulta Tipi di risorsa supportati. Questa versione supporta due nuove regole gestite: • redshift-cluster-configuration-check • redshift-cluster-maintenancesettings-check Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	7 dicembre 2016
Contenuti nuovi e aggiornati	Questa versione aggiunge il supporto per una nuova regola gestita: • dynamodb-throughput-limit-check Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	7 dicembre 2016

Modifica	Descrizione	Data di rilascio
Contenuti nuovi e aggiornati	Questa versione aggiunge il supporto per la creazione di un massimo di 50 regole per regione in un account. Per ulteriori informazioni, consulta Limiti di configurazione di AWS nei Riferimenti generali di AWS.	7 dicembre 2016
AWS Config supporta il tipo di risorsa di inventario delle istanze gestite per Amazon EC2 Systems Manager e tre nuove regole gestite	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione del software sulle istanze gestite con supporto per l'inventario delle istanze gestite. Per ulteriori informazioni, consulta Recording Software Configuration for Managed Instances. Questa versione supporta tre nuove regole gestite: • ec2-managedinstance-inventory-blacklisted • ec2-managedinstance-applications-required • ec2-managedinstance-platform-check Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	1 dicembre 2016

Modifica	Descrizione	Data di rilascio
AWS Config supporta la risorsa bucket Amazon S3 e due nuove regole gestite	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione dei tuoi bucket Amazon S3. Per ulteriori informazioni, consulta Tipi di risorsa supportati. Questa versione supporta due nuove regole gestite: • s3-bucket-logging-enabled • s3-bucket-versioning-enabled Per ulteriori informazioni, consulta AWS Config Regole gestite.	18 Ottobre 2016
Contenuti nuovi e aggiornati	Questa versione aggiunge il supporto AWS Config e le AWS Config regole nella regione Stati Uniti orientali (Ohio). Per ulteriori informazioni, consulta Regioni AWS ed endpoint nella Riferimenti generali di AWS.	17 ottobre 2016

Modifica	Descrizione	Data di rilascio
Regole gestite nuove e aggiornate	Questo aggiornamento aggiunge il supporto per otto nuove regole gestite: • approved-amis-by-id • approved-amis-by-tag • db-instance-backup-enabled • desired-instance-type • ebs-optimized-instance • iam-password-policy • rds-multi-az-support • rds-storage-encrypted Puoi specificare più valori di parametro per le seguenti regole: • desired-instance-tenancy • required-tags Per ulteriori informazioni, consulta Elenco di regole AWS Config gestite.	4 Ottobre 2016

Modifica	Descrizione	Data di rilascio
Contenuti nuovi e aggiornati per la console AWS Config	Questo aggiornamento aggiunge il supporto per la visualizzazione dell'attività delle AWS CloudTrai l API nella AWS Config timeline. Se stai effettuando CloudTrail la registrazione per il tuo account, puoi visualizzare gli eventi di creazione, aggiornamento ed eliminazione delle API per le modifiche alla configura zione delle tue risorse. Per ulteriori informazioni, consulta Visualizz azione della cronologia di configura zione e conformità.	06 settembre 2016
AWS Config supporta il tipo di risorsa Elastic Load Balancing	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione dei sistemi di bilanciamento del carico delle applicazioni Elastic Load Balancing. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	31 agosto 2016
Contenuti nuovi e aggiornati	Questa versione aggiunge il supporto per AWS Config le regole nelle regioni Asia Pacifico (Singapore) e Asia Pacifico (Sydney). Per ulteriori informazioni, consulta Regioni AWS ed endpoint nella Riferimenti generali di AWS.	18 agosto 2016

Modifica	Descrizione	Data di rilascio
Contenuti nuovi e aggiornati per AWS Config le Regole	Questo aggiornamento aggiunge il supporto per la creazione di una regola che può essere attivata da entrambe le modifiche di configura zione e con una frequenza periodica che puoi selezionare. Per ulteriori informazioni, consulta Modalità di valutazione e tipi di trigger per AWS Config le regole. Inoltre, l'aggiornamento aggiunge il supporto per la valutazione manuale delle risorse a fronte della regola e consente di eliminare i risultati della valutazione. Per ulteriori informazi oni, consulta Valutare le risorse con le regole AWS Config. Inoltre, l'aggiornamento aggiunge il supporto per valutare ulteriori tipi di risorse utilizzando regole personali zzate. Per ulteriori informazioni, consulta Valutazione tipi di risorse aggiuntive.	25 luglio 2016

Modifica	Descrizione	Data di rilascio
AWS Config supporta i tipi di risorse Amazon RDS e AWS Certificate Manager (ACM)	Con questa versione, puoi utilizzar e AWS Config per registrare le modifiche alla configurazione delle istanze DB di Amazon Relational Database Service (Amazon RDS), dei gruppi di sicurezza DB, degli snapshot DB, dei sottoreti DB e degli abbonamenti a eventi. Puoi anche utilizzarlo AWS Config per registrare le modifiche alla configurazione dei certificati forniti da ACM. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	21 luglio 2016
Aggiornam ento delle informazioni sulla gestione del registratore della configura zione	Questo aggiornamento aggiunge a Gestione del registratore della configurazione una serie di passaggi per la ridenominazione e l'elimina zione del registratore per la configura zione.	07 luglio 2016

Modifica	Descrizione	Data di rilascio
Semplificazione della procedura di creazione ruoli e policy aggiornate	Con questo aggiornamento, la creazione di un ruolo IAM per AWS Config è semplificata. Questa funzione sarà disponibile in tutte le regioni che supportano le regole Config. Per supportare questa funzione, si è provveduto all'aggio rnamento delle istruzioni in Configura zione AWS Config con la console, della policy di esempio di Autorizza zioni per il bucket Amazon S3 per il canale di distribuzione AWS Config e della policy di esempio di Esempi di policy basate sull'identità per AWS Config.	31 marzo 2016
Funzioni ed eventi di esempio per le regole Config	Questo aggiornamento fornisce nuove funzioni di esempio in AWS Lambda Funzioni di esempio per AWS Config le regole (Node.js) e aggiunge eventi di esempio in Esempio eventi per le regole AWS Config.	29 marzo 2016
AWS Config Archivio delle regole GitHub	Questo aggiornamento aggiunge informazioni sul GitHub repository AWS Config Rules a. Valutazione delle risorse con regole AWS Config Questo repository fornisce funzioni di esempio per regole personalizzate sviluppate e fornite dagli AWS Config utenti.	1 marzo 2016

Modifica	Descrizione	Data di rilascio
AWS Config Regole	Questa versione introduce AWS Config le regole. Le regole possono essere utilizzate AWS Config per valutare se le AWS risorse sono conformi alle configurazioni desiderate. Per ulteriori informazioni, consulta Valutazione delle risorse con regole AWS Config.	18 dicembre 2015
AWS Config supporta i tipi di risorse IAM	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione degli utenti, dei gruppi, dei ruoli e delle policy gestite dai clienti di IAM. Per ulteriori informazioni, consultare Tipi di risorsa supportati.	10 dicembre 2015
AWS Config supporta l'host dedicato EC2	Con questa versione, puoi utilizzar la AWS Config per registrare le modifiche alla configurazione dei tuoi host dedicati EC2. Per ulteriori informazioni, consulta Tipi di risorsa supportati.	23 novembre 2015

Modifica	Descrizione	Data di rilascio
Aggiornamento delle informazioni sulle autorizzazioni	Questo aggiornamento aggiunge informazioni sulle seguenti politiche AWS gestite per AWS Config: • `AWS_ConfigRole` : concede a AWS Config l'autorizzazione per ottenere i dettagli di configurazione sulle risorse. Per ulteriori informazioni, consulta Policy del ruolo IAM per il recupero dei dettagli di configurazione. • `AWSConfigUserAccess` — Concede l'accesso in sola lettura a un utente. AWS Config Per ulteriori informazioni, consulta Accesso in sola lettura a AWS Config.	19 ottobre 2015
AWS Config Anteprima delle regole	Questa versione introduce l'anteprima delle AWS Config regole. Le regole possono essere utilizzate AWS Config per valutare se le AWS risorse sono conformi alle configurazioni desiderate. Per ulteriori informazioni, consulta Valutazione delle risorse con regole AWS Config.	7 Ottobre 2015
Contenuti nuovi e aggiornati	Questa versione aggiunge la possibilità di cercare le AWS Config risorse scoperte. Per ulteriori informazioni, consulta Ricerca di risorse scoperte da AWS Config.	27 agosto 2015

Modifica	Descrizione	Data di rilascio
Contenuti nuovi e aggiornati	Questa versione aggiunge la possibilità di selezionare quali tipi di risorse devono essere registrate da AWS Config . Per ulteriori informazioni, consulta AWS Risorse per la registrazione.	23 giugno 2015
Contenuti nuovi e aggiornati	Questo rilascio aggiunge il supporto per le seguenti regioni: Asia Pacifico (Tokyo), Asia Pacifico (Singapore), Europa (Francoforte), Sud America (San Paolo) e Stati Uniti occidentali (California settentrionale). Per ulteriori informazioni, consulta Regioni AWS ed endpoint.	6 Aprile 2015
Nuova guida	Questa versione introduce AWS Config.	12 novembre 2014

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.